

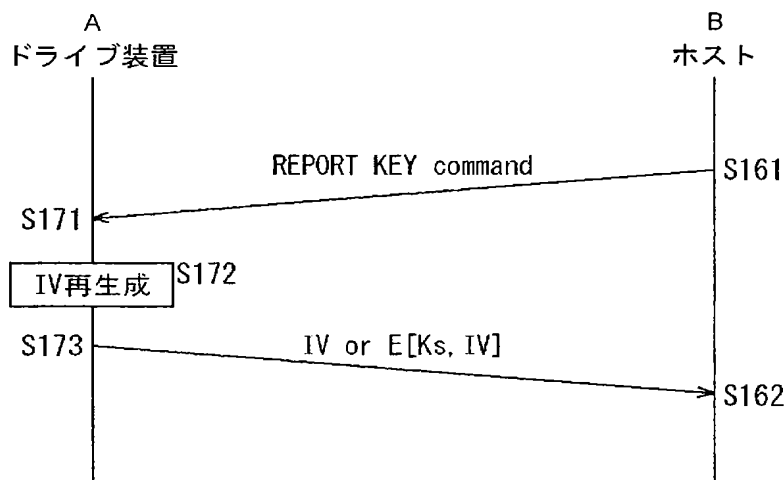


**PCT**

**RESEARCH DESIGN**

- 〔続葉有〕

(54) 発明の名称: 情報処理装置



A DRIVE DEVICE  
B HOST  
S172 IV REPRODUCTION

**(57) Abstract:** There are provided an information processing device and method, program, and recording medium capable of transmitting/receiving data with a high security. A host is connected to a drive device by a predetermined bus, via which data is transmitted and received. The host periodically requests the drive device to issue an initial vector IV used for encryption and decryption of data transmitted and received via the bus. When the drive device has received the request, it generates the initial vector IV and supplies it to the host. If such a process is not performed periodically, the drive device stops data output to the host. The present invention can be applied to a personal computer having a drive device for reproducing data recorded on a recording medium.

(57) 要約: 本発明は、データの授受をセキュリティを高めた状態で行えるようにする情報処理装置および方法、プログラム、並びに記録媒体に関する。ホストとドライブ装置は、所定のバス

〔続葉有〕

WO 2005/067198 A1



SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,  
VC, VN, YU, ZA, ZM, ZW.

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,  
MR, NE, SN, TD, TG).

(84) 指定国 (表示のない限り、全ての種類の広域保護  
が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA,  
SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ,  
BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE,  
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,  
IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR),

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される  
各PCTガゼットの巻頭に掲載されている「コードと略語  
のガイダンスノート」を参照。

で接続されており、そのバスを介してデータの授受を行う。ホストは、ドライブ装置に対して、バス上を介して授受されるデータを暗号化および復号の際に用いられる初期ベクトルIVの発行の要求を定期的に行う。ドライブ装置は、要求があったとき、初期ベクトルIVを生成しホストに供給する。このような処理が定期的に行われなければ、ドライブ装置は、ホストに対するデータの出力を停止する。本発明は、記録媒体に記録されているデータを再生するドライブ装置を有するパーソナルコンピュータに適用することが可能である。

## 明 細 書

### 情報処理装置

#### 技術分野

- [0001] 本発明は、情報処理装置および方法、プログラム、並びに記録媒体に関し、特に、暗号化に関わる処理を実行する際に用いて好適な情報処理装置および方法、プログラム、並びに記録媒体に関する。

#### 背景技術

- [0002] さまざまな装置で、デジタルデータを授受することが一般的になりつつあるが、デジタルデータは、不正に利用されても、その質(例えば、画質や音質)が劣化しないため、不正に利用されないための対策が必要とされる。(例えば、特許文献1参照)
- [0003] また近年普及しつつあるDVD(Digital Versatile Disc)等の記録媒体では、1枚の記録媒体(ディスク)に、例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると、不正なコピーを防止して著作権者の保護を図ることが益々重要になってくる。
- [0004] そこで、例えば、DVDにビデオコンテンツを格納したDVDビデオでは、著作権保護技術として、CSS(Content Scramble System)方式が採用されている。図1は、CSS方式を用いて暗号化されたデータが記録されている記録媒体と、その記録媒体を再生する装置の構成の一例を示す図である。
- [0005] 図1においては、記録媒体として、ディスク11を例に挙げて図示してある。ディスク11には、ディスク11を識別するためのディスクキー(Secured Disc Key)21、記録されているデータの所定の単位毎に設けられているタイトルキー(Encrypted Title Key)22、および、データ(Scrambled Data)23が記録されている。タイトルキー22は、例えば、ディスク11に映画が記録されているような場合、チャプター(Chapter)毎に設けられる。
- [0006] ディスクキー21とタイトルキー22は、暗号化された状態(または、容易に読み出すことが(盗用することが)できない状態)でディスク11に記録されている。また、データ23

は、タイトルキー22を用いたスクランブル(Scramble)がかけられた状態でディスク11に記録されている。

- [0007] プレーヤ12は、ディスク11に記録されているキーやデータを読み出すことにより、データ23の再生を行う。プレーヤ23は、復号(Decrypt)部32、復号部33、デスクランブル(DeScramble)部34、および、デコーダ(Decoder)35を有する構成とされている。また、プレーヤ12は、マスタキー(Master Key)31を管理する管理部(不図示)も有している。
- [0008] 復号部32は、ディスク11から読み出されたディスクキー21を、マスタキー31を用いて復号し、その復号したディスクキー21を復号部33に供給する。復号部33には、ディスク11から読み出されたタイトルキー22も供給される。復号部33は、復号されたディスクキー21により、暗号化されているタイトルキー22を復号する。復号されたタイトルキー22は、デスクランブル部34に供給される。デスクランブル部34には、ディスク11から読み出されたデータ23も供給される。
- [0009] ディスク11から読み出され、プレーヤ12に供給されるデータ23は、所定の圧縮方式(例えば、MPEG (Moving Picture Expert Group) 方式)で圧縮され、さらにタイトルキー22を用いたスクランブルがかけられた状態のものである。そこで、まず、デスクランブル部34は、タイトルキー22を用いて、データ23にかけられているスクランブルを解除する。
- [0010] スクランブルが解除されたデータ23は、デコーダ35に供給される。デコーダ35は、所定のデコード方式(例えば、MPEG方式)により、デスクランブル部34からのデータ23をデコードする。デコードされたデータ36は、図示されていないディスプレイなどに供給される。
- [0011] 図1に示したプレーヤ12は、例えば、DVDなどのディスク11を専用に再生するような機器であるが、そのような専用のプレーヤ12に限らず、例えば、パーソナルコンピュータなどもディスク11を再生する機能を有している場合がある。
- [0012] 図2は、DVDなどのディスク11をパーソナルコンピュータなどで再生する場合の構成例を示す図である。ここでは、ディスク11に記録されているデータを読み出す装置をドライブ装置51とし、ドライブ装置51により読み出されたデータを処理する装置を

ホスト(Host)52と記述する。図2に示したドライブ装置51やホスト52には、アプリケーションなどにより実現される機能も含まれている。

- [0013] ディスク11には、図1に示した場合と同様に、ディスクキー21、タイトルキー22、および、データ23が記録されている。ドライブ装置51は、認証(Authentication)処理部62、バス暗号化(Bus Encrypt)部62、および、バス暗号化部63を有する構成とされている。
- [0014] ホスト52は、認証処理部71、バス復号(Bus Decrypt)部72、バス復号部73、復号(Decrypt)部74、復号部75、デスクランブル部76、および、デコーダ77を有する構成とされている。また、ホスト52は、マスタキー31を管理する管理部(不図示)も有している。
- [0015] ドライブ装置51の認証処理部51とホスト52の認証処理部71は、相互認証処理を実行し、その認証処理が正常に行われたときだけ、データの授受を行う。認証処理が正常に行われると、セッションキーと称されるキーが、それぞれの認証処理部61、71において発行(共用)される。
- [0016] 認証処理が正常に行われた後の時点で、ディスク11から読み出されたディスクキー21は、ドライブ装置51のバス暗号化部62により暗号化される。バス暗号化部62には、認証処理部61において発行されたセッションキーも供給される。バス暗号化部62は、読み出されたディスクキー21を、セッションキーを用いて暗号化し、ホスト71に対して出力する。
- [0017] 同様に、バス暗号化部63は、ディスク11から読み出されたタイトルキー22を、認証処理部61が発行したセッションキーを用いて暗号化し、ホスト52に対して出力する。ディスク11から読み出されたデータ23は、直接的に、ドライブ装置51からホスト52に対して供給される。
- [0018] ホスト52のバス復号部72は、ドライブ装置51のバス暗号化部62から供給された暗号化されているディスクキー21を、認証処理部71により発行されたセッションキーを用いて復号する。復号されたディスクキー21は、復号部74に供給される。復号部74には、マスタキー31も供給される。復号部74は、バス復号部72から供給されたディスクキー21を、マスタキー31を用いて復号し、その復号したディスクキー21を復号部7

5に供給する。

- [0019] 復号部75には、バス復号部73からのタイトルキー22も供給されるが、そのタイトルキー22は、バス復号部73が、認証処理部71により発行されたセッションキーを用いて復号したものである。
- [0020] 復号部75は、復号されたディスクキー21により、暗号化されているタイトルキー22を復号する。復号されたタイトルキー22は、デスクランブル部76に供給される。デスクランブル部76には、ディスク11から読み出されたデータ23も供給される。
- [0021] ディスク11から読み出されるデータ23は、所定の圧縮方式で圧縮され、さらにタイトルキー22を用いたスクランブルがかけられた状態のものである。そこでまず、デスクランブル部76は、供給されたタイトルキー22を用いて、データ23にかけられているスクランブルを解除する。
- [0022] スクランブルが解除されたデータ23は、デコーダ77に供給される。デコーダ77は、所定のデコード方式(例えば、MPEG方式)により、供給されたデータ23をデコードする。デコードされたデータ36は、図示されていないディスプレイなどに供給される。
- [0023] このように、ディスク11がセットされるドライブ装置51と、ディスク11に記録されているデータを処理するホスト52により、ディスク11に記録されているデータ23の再生の処理が実行される場合、認証処理が行われ、その認証処理が正常に行われた後に、暗号化されたキーやデータの授受が行われる。
- [0024] 認証処理が行われた後に、実際のデータの授受が行われるのは、ドライブ装置51とホスト52は、所定のバス(不図示)により接続されているが、そのバスを介して授受されるデータが盗用されないようにするためである。
- [0025] ここで、認証処理部61と認証処理部71との間で行われる認証処理について、図3のフローチャートを参照して説明を加える。ステップS11において、ディスク11が、ドライブ装置51に挿入(セット)されたか否かが判断される。ステップS11において、ディスク11が、ドライブ装置51に挿入されたと判断されるまで、待機状態が維持される(ステップS11における処理が繰り返される)。
- [0026] ステップS11において、ディスク11が、ドライブ装置51に挿入されたと判断された場合、ステップS12に処理が進められる。ステップS12において、認証処理部61と認証

処理部71により、相互認証の処理が実行される。この相互認証の処理が正常に終了されなければ、これ以降の処理は実行されない。

- [0027] 相互認証の処理が正常に終了されると、認証処理部61と認証処理部71のそれぞれにおいて、セッションキーが生成される。このような相互認証の処理とセッションキーの発生処理が完了したか否かが、ステップS13において判断される。ステップS13において、ステップS12における処理は完了したと判断されるまで、ステップS12の処理が繰り返され、完了したと判断された場合、ステップS14に処理が進められる。
- [0028] ステップS14において、スクランブルされたデータの授受(ドライブ装置51からの出力)が許可された状態に設定される。この場合、スクランブルされたデータとは、データ23(図2)のことであり、このデータ23のドライブ装置51からホスト52への出力が許可された状態に設定される。
- [0029] “許可された状態”ということについて説明を加える。データ23の読み出しは、ホスト52からの指示に基づいてドライブ装置51が行う。許可される前の状態において、ドライブ装置51は、仮にホスト52からデータ23の読み出し(出力)の指示を受けたとしても、エラーを返すだけで、データ23の出力は行わない。
- [0030] 許可された後の状態においては、ホスト52からデータ23の読み出した指示されれば、ドライブ装置51は、ディスク11からデータ23を読み出し、ホスト52に対して出力を行う。
- [0031] このような状態に設定されると、ディスク11がドライブ装置51から排出されるなどの割り込み処理が発生しない限り、スクランブルされたデータ23の再生の処理が繰り返し行われる。
- [0032] スクランブルされたデータ23の出力が許可された状態にされると、ステップS15において、ディスク11がドライブ装置51から排出された否かの判断が継続的に行われる。そして、ステップS15において、ディスク11がドライブ装置51から排出されたと判断されると、ステップS11に処理が戻され、それ以降の処理が繰り返される。
- [0033] なお、ドライブがリセットされた場合や、電源がオフの状態にされた場合も、再生の処理が終了され、必要に応じ、ステップS11に処理が戻され、それ以降の処理が繰り返される。

返される。

- [0034] このようにして、ドライブ装置51とホスト52との間で認証処理が正常に終了されると、ドライブ装置51側では、ディスク11が排出されるまで、その挿入されているディスク11からデータ23を読み出し、その読み出したデータ23をホスト52に出力するという処理を、ホスト52からの指示がある限り継続的に行なわれる。
- [0035] ここで、バス暗号化部62などの暗号化部において行われる公知の暗号化技術について説明を加える。暗号化の方式は、さまざまなものが提案されている。ここでは、CBC (Cipher Block Chaining) 方式を例に挙げて、暗号化(復号)の方式について説明する。
- [0036] 暗号化の一方式であるCBC方式は、ブロック連鎖のための一つの技法であり、排他的論理和演算により、平文の現在のブロックに暗号文の前のブロックを付加して、暗号文の各ブロックを作成する方式である。図4は、CBC方式を用い暗号化を行う回路の一例を示す図である。
- [0037] 暗号化すべきデータは、所定の単位(例えば、ブロック暗号方式としてAES (Advanced Encryption Standard)を用いた場合は16バイト)毎にブロック化される。そして、第1のブロックは、排他的論理和回路101-1に供給され、第1のブロックに続く第2のブロックは、排他的論理和回路101-2に供給され、第2のブロックに続く第3のブロックは、排他的論理和回路101-3に供給されというように、所定の段数(ここでは、N段とする)だけ設けられた排他的論理和回路101-1乃至101-Nに順次、ブロック化された平文のデータが入力される。
- [0038] 排他的論理和回路101-1から出力された第1のブロックは、暗号化部102-1に供給される。暗号化部102-1は、鍵 $E_k$ で供給された第1のブロックを暗号化する。このようにして、第1のブロックは暗号化される。
- [0039] 暗号化部102-1から出力された暗号化された第1のブロックは、排他的論理和回路101-2にも供給され、第2のブロックとの間で排他的論理和が演算される。その結果は、暗号化部102-2に供給され、同じく鍵 $E_k$ で暗号化される。
- [0040] このように、CBC方式における暗号化は、1つ前で暗号化したブロックと暗号化対象の現在の平文のブロックとの排他的論理和が演算されてから、そのブロックに対し



て所定の暗号化鍵での暗号化が行なわれるようになっている。結果の暗号文は次のブロックとの排他的論理和の演算に使われることになる。このように前のブロックと次々に連鎖させることにより暗号文が生成される。

- [0041] 第2のブロック以降は、前のブロックとの排他的論理和が演算されるが、第1のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第1のブロックに対しては、初期ベクトル(IV: Initializing Vector)を与えて排他的論理和を演算するように構成される。
- [0042] 次に、CBC方式を用い復号を行う回路(例えば、バス復号部72(図2))について、図5を参照して説明する。
- [0043] 上述したようにして暗号化されたデータは、所定の単位(例えば、ブロック暗号方式としてAES(Advanced Encryption Standard)を用いた場合は16バイト)毎にブロック化されている。ブロック化されているデータの内、第1のブロックは、復号部122-1に供給され、第1のブロックに続く第2のブロックは、復号部122-2に供給され、第2のブロックに続く第3のブロックは、復号部122-3に供給されというように、所定の段数(ここでは、N段とする)だけ設けられた復号部122-1乃至122-Nに順次、暗号化されたブロック単位のデータが入力される。
- [0044] 各復号部122-1乃至122-Nは、入力されたデータを鍵Dkで復号する。各復号部122-1乃至122-Nから出力されたデータは、対応する排他的論理和回路121-1乃至121-Nに供給される。排他的論理和回路121-2乃至121-Nには、前の段の復号部122-1乃至122-N-1に供給されるデータも供給される。
- [0045] このように、CBC方式の復号は、1つ前の暗号化されているブロックと復号対象の現在の復号されたブロックとの排他的論理和が演算されることにより、最終的な復号が行われる。
- [0046] 第2のブロック以降は、前のブロックとの排他的論理和が演算されるが、第1のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第1のブロックに対しては、初期ベクトルIVを与えて、排他的論理和が演算される構成とされている。
- [0047] このようにして、暗号化、復号が行われている。

特許文献1:特許第3252706号明細書

発明の開示

発明が解決しようとする課題

- [0048]   ところで、図2に示したように、ドライブ装置51とホスト52によりディスク11に記録されているデータ23の再生の処理が実行される場合、図3のフローチャートを参照して説明したように、ドライブ装置51とホスト52における相互認証の処理が正常に終了されると、ドライブ装置51からのデータ23の出力が許可された状態にされる。
- [0049]   ここで、図6を参照して説明するに、ホスト52側でアプリケーションAが起動され、そのアプリケーションAにより、認証処理部71で行う認証処理が実行される場合を考える。アプリケーションAによるドライブ装置51との認証処理が正常に実行されると、ドライブ装置51からディスク11からデータ23が読み出され、出力されるといった処理が許可された状態にされる。
- [0050]   許可された状態のときに、ディスク11がドライブ装置51から排出されるなどの状況が発生しない限り、ドライブ装置51からデータ23が出力されるといった処理が許可された状態が維持される。そのような許可が維持されている状態のときに、アプリケーションBがホスト52側で起動されたとする。そして、アプリケーションAにかわり、アプリケーションBにより、データ23の読み出しの指示などの処理が開始されたとする。
- [0051]   ドライブ装置51とアプリケーションBは、認証処理を行っていないにもかかわらず、ドライブ装置51は、データ23の出力が許可された状態に維持されているため、ドライブ装置51からホスト52(アプリケーションB)に対して、データ23は出力されてしまう。その結果、例えば、ホスト52が有するHDD(Hard Disc Drive)141にデータ23が記憶されるといった処理が、アプリケーションBにより実行される可能性がある。
- [0052]   このHDD141に対するデータ23の記憶が不正な処理であっても、ドライブ装置51は、アプリケーションBの指示に基づき、データ23を出力してしまう。よって、このような不正を防ぐことができないといった課題があった。
- [0053]   また、HDD141に記憶されたデータ23は、スクランブルがかけられた状態であるため、そのままでは再生することができないが、スクランブルを解除するアプリケーションなども存在しているため、実質的には、HDD141にデータ23が記憶された時点で、

不正に利用されてしまうことを防ぐことができないといった課題があった。

[0054] このように、一旦、正常に認証処理が行われ、ドライブ装置51側でデータ23の出力が許可された状態にされると、データ23が盗用されてしまう可能性があるといった課題があった。

[0055] 図7を参照し、他のデータの盗用について説明する。ドライブ装置51とホスト52は、所定のバスにより接続され、そのバスを介してデータ23の授受を行うように構成されている。図6を参照して説明した場合と同様に、アプリケーションAにより、ドライブ装置51との認証処理が行われる。そして、その認証処理が正常に行われると、ドライブ装置51からデータ23を出力するといった処理を実行することが許可された状態とされる。

[0056] バス上を授受されるデータをモニタする機能をホスト52が有していると、そのモニタ151により、バス上で授受されているデータ23をモニタする(取得する)ことが可能である。換言すれば、ドライブ装置51から出力されたデータ23は、アプリケーションAとモニタ151に供給されるといった状態にすることが可能である。

[0057] そのため、ホスト52側で、モニタ151により取得されたデータ23を、HDD141に記憶させるといった処理を実行することも可能となる。よって、このようにしてデータ23が盗用されてしまう可能性もある。

[0058] このように、バス上を授受されるデータが、モニタ機能により盗用されてしまう可能性があるといった課題があった。

[0059] バス上のデータが盗用されてしまうようなことを防ぐために、バスを介して授受されるデータ23を暗号化する方法も提案されている。図8を参照して説明する。ドライブ装置51側からホスト52に出力されるデータを転送データ171と記述する。

[0060] 転送データ171は、2048バイト(2Kバイト)のデータパケット(data Packet)とされる。上述したように、ドライブ装置51とホスト52は、所定のバスで接続されているわけだが、そのバスをコントロールするバスインタフェース183は、所定の単位量のデータを取り扱うように規定されている。その単位量は、例えば、ATAPI(AT Attachment with Packet Interface)をバスインタフェース183として用いた場合、2048バイトと規定されている。

- [0061] そこで、転送データ171を2048バイトで構成されるデータパケットとした場合、図8に示すように、1パケットは、16バイトの初期ベクトルIVと2032バイトのデータから構成される。このようなデータパケットのうち、2032バイトのデータ部分が、暗号化部181により暗号化される。暗号化部181は、図8には図示していないが、認証処理部181(図2)により発行されるセッションキーKsを用いて暗号化を行う。
- [0062] 暗号化部181は、例えば、CBC方式を用いて暗号化を行う。CBC方式に基づいて暗号化を行う場合、暗号化部181の内部構成例は、図4に示したようになる。図4を参照して説明したように、暗号化部181は、初期ベクトルIVも用いて暗号化を行う。すなわち、暗号化部181は、転送データ171のデータパケットの内、2038バイトのデータ部分を、同じくデータパケット内に含まれる16バイトの初期ベクトルIVと、認証処理部181により発行されるセッションキーKsを用いて暗号化を行う。
- [0063] 暗号化部181により暗号化されたデータパケットも、2048バイトのデータである。よって、その暗号化されたデータパケットは、バスインタフェース183により取り扱うことができる。データ部分が暗号化されたデータパケットは、ホスト52側の復号部182に供給される。復号部182は、供給されたデータパケットに含まれる初期ベクトルIVと、認証処理部71(図2)により発行されるセッションキーKsを用いて、暗号化されているデータの復号を行う。
- [0064] このようにして、ホスト52側は、暗号化されたデータを受信するが、そのデータと共に供給される初期ベクトルIVを用いて復号することができるため、ホスト52側において、ドライブ装置51側から出力されたデータを再生することができる。
- [0065] このように、バスインタフェース183上で授受されるデータを、暗号化されたデータとすることにより、仮に、バスインタフェース183を介して授受されるデータが盗聴されても、暗号化を解くことができなければ、盗用されることがなく、結果として、データが不正に利用されるような不都合が発生するようなことを防ぐことが可能となる。しかしながら、以下のような問題点がある。
- [0066] 再度、図8を参照するに、初期ベクトルIVは、転送データ171に含まれている。転送データ171に初期ベクトルIVを含ませる場合、ディスク11に、他のデータと共に書き込まれている。よって、初期ベクトルIVをランダムに変化させることができない(書き

込まれている初期ベクトルIVをそのまま用いなくてはならず、変化させることができない)といった問題があった。

- [0067] また、ディスク11に初期ベクトルIVが書き込まれているのではなく、ドライブ装置51側でランダムに初期ベクトルIVを発生させ、その初期ベクトルIVを転送データ171内に含ませるようにすることも考えられ。しかしながら、転送データ171に初期ベクトルIVが含ませる場合、暗号化されるデータと区別するために、例えば、ヘッダなどを付けなくてはならないなどの条件がある。
- [0068] そのような条件があるために、ドライブ装置51側で、ランダムに初期ベクトルIVを発生させるようにしても、ランダムに変化させることに対する制限があり、結果的には、ランダムに初期ベクトルIVを発生させるということに対してそのランダム性を保証することができない(固定パターンになってしまう)といった問題があった。
- [0069] 初期ベクトルIVをランダムに変化させることができない場合、換言すれば、初期ベクトルIVとして固定パターンが用いられるようにすると、以下のような問題が発生する可能性がある。
- [0070] 例えば、電子メールを例に挙げて考える。電子メールの書式には、宛先、送信元、件名、本文といったような一連のパターンがある。そのようなパターンがあるようなデータ(平文)を暗号化した場合、暗号化されたデータ自体もパターンがあるデータになってしまう。第3者(攻撃者)が、そのようなパターンに注目することにより、暗号文から平文の一部を解読することが可能である。
- [0071] また、音楽データなどで、その音楽データを繰り返し再生するような場合、結果として同じ平文を同じように暗号化することになり、暗号化されたデータ自体も同じ結果となる。そのため、上述した場合と同様に、暗号文から平文を解読することが可能である。
- [0072] そこで、パターンがあるような平文(同一のデータを複数回暗号化するような場合)でも、暗号化されたデータ(暗号文)にパターンがないようにするために、最初のブロックに初期ベクトルIVを加えるようにする。初期ベクトルIVを加えて暗号化を実行することにより、平文のブロックに同じパターンがあっても暗号文には同じパターンが発生しないので、暗号解読を困難にさせることが出来る。また、単一の鍵で大量のデー

タを暗号化した場合に暗号鍵が予測しやすくなる、という解読行為を、初期ベクトルIVを加えて暗号化を行うようにすることで防止することができるという効果もある。

[0073] このような理由で最初のブロックに初期ベクトルIVが加えられ、その後の暗号化が行われるように構成されている場合が多い。

[0074] そして、初期ベクトルIVを適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができるとされている。(参考文献:NIST Special Publication 800-38A 2001 Edition, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, APPENDIX C Generation of Counter Blocks)

[0075] よって、同じ初期ベクトルIVが繰り返し用いられると、結果として、初期ベクトルIVを適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができないといった課題があった。

[0076] また、上述したように、初期ベクトルIVは、更新される方が好ましいといった課題があった。

[0077] そこで、初期ベクトルIVを更新できるようにした場合、図9に示すようなデータの授受の方法が考えられる。すなわち、図9に示した例では、転送データ191は、2048バイトのデータから構成され、そのデータに、16バイトの初期ベクトルIVが付加される。そして、初期ベクトルIVが付加された結果、2064バイトにされたデータが、バスインタフェース183を介して授受される。

[0078] 初期ベクトルIVを転送データ191に付加する構成とすることにより(転送データ191に初期ベクトルIVを予め含めるような構成としないことにより)、初期ベクトルIVを、ドライブ装置51側でランダムに発生し、そのランダムに発生された初期ベクトルIVを付加させることができるようになる。

[0079] しかしながら、このようにして初期ベクトルIVをデータに付加することは、例えば 2048バイト単位のPC Drive Interface に、2064バイト(IV=16バイトの場合)という特殊なセクタサイズを持ち込むことになり、標準的なフォーマットから外れてしまうこととなる。そのために、共通の ATAPI Device Driver を利用できない、UDF(Universal Data

Format)で扱うことのできるセクタサイズである2048バイトや4096バイトに当てはまらないためUDF FS Driverを利用できないなど、パーソナルコンピュータにおける環境との相性がよくないといった課題があった。

[0080] 相性が良くないといったことを解決するためには、ハードウェア的に、ソフトウェア的にも特殊なものに変えなくてはならないなど、コスト的に割高になり、互換性を取りづら、処理的に手間がかかるといった課題もあった。

[0081] 本発明はこのような状況に鑑みてなされたものであり、認証処理が正常に終了し、ドライブ装置側からデータが出力されることが許可された状態にされた後においても、その許可状態を解除できるようにし、データの盗用を防ぐことを目的とする。また、汎用なバスを用いた場合においても、初期ベクトルIVを更新できるようにし、そのバス上で授受されるデータが盗用されないようなセキュリティを高めることを目的とする。

#### 課題を解決するための手段

[0082] 本発明の情報処理装置は、データの転送を制御する転送制御手段と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断手段と、第1の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第1の指示手段と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断手段と、第2の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウンタ手段によりカウントされている回数をリセットするように指示を出す第2の指示手段とを備えることを特徴とする。

[0083] 前記第1の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段をさらに備えるようにすることができる。

[0084] 本発明の情報処理方法は、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと

、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含むことを特徴とする。

[0085] 本発明のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含む処理をコンピュータに実行させることを特徴とする。

[0086] 本発明の記録媒体のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値



以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含むことを特徴とする。

- [0087] 本発明の情報処理装置および方法、並びにプログラムにおいては、初期ベクトルの供給の指示が定期的に行われなければ、データの授受が停止される。

#### 発明の効果

- [0088] 本発明によれば、装置間での転送路上におけるセキュリティを高めることが可能となる。
- [0089] また、本発明によれば、記録媒体を扱う装置とその装置からのデータを扱う他の装置との間で認証処理が行われた後、記録媒体を扱う装置側で、記録媒体から読み出したデータを他の装置に出力することが許可された状態にされても、その状態を解除（更新）することが可能となる。もって、一旦、他の装置へのデータの出力が許可された状態であっても、その後の不正なアクセスによるデータの流出を防ぐことが可能となる。
- [0090] また、本発明によれば、暗号化の際に用いられる初期ベクトルをランダムに更新することができ、同一のデータを暗号化しても、同一の暗号文が生成されるようなことを防ぐことが可能となる。もってデータのすり替え、データの改竄行為などの不正な処理を防止することができる。
- [0091] また、本発明によれば、初期ベクトルを更新するようにしても、汎用のバスインタフェースおよびOS(Operating System)で標準的に用意されたUDF FS Driverを利用できる。もって、初期ベクトルを更新できるようにするために、装置間の環境を変更しなくてはならないといったような不都合が発生するようなことを防ぐことができる。

## 図面の簡単な説明

- [0092] [図1]従来の再生装置の一例の構成を示す図である。
- [図2]従来の再生装置の他の構成例を示す図である。
- [図3]認証処理について説明するためのフローチャートである。
- [図4]暗号化を行う回路の構成例を示す図である。
- [図5]復号を行う回路の構成例を示す図である。
- [図6]従来の再生装置における問題点を説明するための図である。
- [図7]従来の再生装置における問題点を説明するための図である。
- [図8]初期ベクトルIVを授受する際の問題点を説明するための図である。
- [図9]初期ベクトルIVを授受する際の問題点を説明するための図である。
- [図10]本発明を適用したシステムの一実施の形態の構成を示す図である。
- [図11]データの授受に係わるドライバーについて説明するための図である。
- [図12]ドライブ装置の動作について説明するためのフローチャートである。
- [図13]図12のフローチャートに続くフローチャートである。
- [図14]初期ベクトルIVの授受に関するタイミングチャートである。
- [図15]初期ベクトルIVの授受に関するタイミングチャートである。
- [図16]初期ベクトルIVの授受に関するタイミングチャートである。
- [図17]データの授受に関するタイミングチャートである。
- [図18]コマンドパケットの構成を示す図である。
- [図19]本発明を適用したシステムの他の実施の形態の構成を示す図である。
- [図20]データの授受に関するタイミングチャートである。
- [図21]実施例2における記録装置の構成を示す図である。
- [図22]初期ベクトルIVの授受に関するタイミングチャートである。
- [図23]初期ベクトルIVの授受に関するタイミングチャートである。
- [図24]ホストの動作について説明するためのフローチャートである。
- [図25]図24のフローチャートに続くフローチャートである。
- [図26]ドライブ装置の動作について説明するためのフローチャートである。
- [図27]図26のフローチャートに続くフローチャートである。

## 符号の説明

[0093] 301 ドライブ装置, 302 ホスト, 303 ディスク, 311 認証処理部, 312 暗号化部, 313 セクタ転送制御部, 314 セクタ転送カウンタ, 315 乱数発生部, 316 メッセージ伝達部, 317 コマンド処理部, 318 アクセス処理部, 321 認証処理部, 322 復号部, 401 ドライブ装置, 402 ホスト, 403 ディスク, 411 認証処理部, 412 復号部, 413 セクタ転送制御部, 414 セクタ転送カウンタ, 415 乱数発生部, 416 メッセージ伝達部, 417 コマンド処理部, 418 アクセス処理部, 421 認証処理部, 422 暗号化部

## 発明を実施するための最良の形態

[0094] 以下に本発明の最良の形態を説明するが、開示される発明と実施の形態との対応関係を例示すると、次のようになる。明細書中には記載されているが、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。

[0095] さらに、この記載は、明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により出現し、追加される発明の存在を否定するものではない。

[0096] 本発明を適用した情報処理装置は、データの転送を制御する転送制御手段(例えば、図13のステップS46の処理を実行する図10のセクタ転送制御部313)と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段(例えば、図13のステップS47の処理を実行する図10のセクタ転送カウンタ314)と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断手段(例えば、図13のステップS45の処理を実行する図10のセクタ転送カウンタ314)と、第1の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第1の指示手段(例えば、図10のセク

タ転送カウンタ314)と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段(例えば、図13のステップS41の処理を実行する図10の乱数発生部315)と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断手段(例えば、図13のステップS40の処理を実行する図10のコマンド処理部317)と、第2の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウンタ手段によりカウントされている回数をリセットするように指示を出す第2の指示手段(例えば、図13のステップS42の処理を実行する図10の乱数発生315)とを少なくとも備える。

[0097] 前記第1の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段(例えば、図13のステップS48の処理を実行する図10のメッセージ伝達部316)をさらに備える。

[0098] 以下に、本発明の実施の形態について図面を参照して説明する。

#### [実施例1]

[0099] 図10は、本発明を適用したシステムの一実施の形態の構成を示す図である。

[0100] 図10に示したシステムは、所定の記録媒体に記録されたデータを再生する(読み出す)システムの構成例を示している。図10に示したシステムは、データを供給するドライブ装置301と、データの供給を受けるホスト302から構成されている。

[0101] ディスク303は、例えば、CD-ROM ( Compact Disc-ROM )、CD-R ( Compact Disc-Recordable )、CD-RW ( Compact Disc-ReWritable )、DVD-ROM ( Digital Versatile Disc-ROM )、DVD-R ( Digital Versatile Disc-Recordable )、DVD-RW ( Digital Versatile Disc-Rerecordable )、DVD+R ( DVD+Recordable )、DVD+RW ( DVD+ReWritable )、DVD-RAM ( Digital Versatile Disk-Random Access Memory )、Blu-Ray Discなどである。また、本発明の適用範囲はこれらの記録媒体に限定されるものではなく、他の形態(記録方式、形状など)の記録媒体を扱うシステムにも適用可能である。

[0102] ドライブ装置301とホスト302は、所定のインタフェースによりデータの授受が行えるように接続されている。所定のインタフェースとしては、例えば、ATAPI ( AT

Attachment with Packet Interface)を用いることができる。ATAPIは、IDE (Integrated Drive Electronics) や、ATA (AT Attachment) インタフェースにCD-ROMドライブなどハードディスク以外の周辺機器を接続するためのデータ転送方式に従ったインタフェースであり、例えばSCSIから流用したコマンドをパケット化してIDEインタフェースに渡すことで周辺機器の制御を可能とする。同様のコマンドパケットはUSB ( Universal Serial Bus ) や IEEE1394 などの物理インタフェースへも適用可能である。

- [0103] ドライブ装置301は、認証処理部311、暗号化部312、セクタ転送制御部313、セクタ転送カウンタ314、乱数発生部315、メッセージ伝達部316、コマンド処理部317、および、アクセス処理部318を含む構成とされている。
- [0104] ホスト302は、認証処理部321、復号部322を含む構成とされている。
- [0105] ドライブ装置301の認証処理部311とホスト302の認証処理部321により、相互認証に関わる処理が実行される。
- [0106] 暗号化部312には、アクセス処理部318による処理により、ディスク303から読み出されたセクタデータ351と、認証処理部311からセッションキーKsが供給される。また、暗号化部312には、乱数発生部315により発生された乱数が、初期ベクトルIVとして供給される。
- [0107] なお、乱数発生部315により発生された乱数を、そのまま初期ベクトルIVとして用いても良いが、乱数と他のデータ(例えば、ディスク303から読み出されるPSN (Physical Sector Number) など) が用いられて生成されるものを初期ベクトルIVとして用いられるようにしても良く、そのような処理を実行する部分を、ドライブ装置301内に設けるようにしても良い。
- [0108] 暗号化部313は、供給されたセクタデータ351をセッションキーKsと初期ベクトルIVを用いて暗号化し、セクタ転送制御部313に供給する。セクタ転送制御部313は、暗号化されたセクタデータ351を、ホスト303の復号部322に対して供給する。  
よって、ドライブ装置301からホスト303に供給されるデータは、暗号化されたセクタデータ351である。
- [0109] 暗号化部312からは、セクタ転送カウンタ314にもデータが出力される。セクタ転送

カウンタ314は、ホスト302に対して出力されたセクタデータ(暗号化部312から出力されたセクタデータ351)の数をカウントするように構成されている。換言すれば、セクタ転送カウンタ314は、セクタ転送制御部313がセクタデータの転送を制御した回数をカウントする。

- [0110] また、セクタ転送カウンタ314は、予め設定されたカウント数の最大値( $N_{\max}$ とする)を管理しており、カウントしているセクタ数(カウンタ値 $N$ )が、その最大値を超えないか否かを常に監視している。
- [0111] セクタ転送カウンタ314は、 $N \geq N_{\max}$ になった場合、セクタ転送制御部313に対して、ホスト302へのセクタデータ351の出力を停止するように指示を出す。このような指示を出すとともに、セクタ転送カウンタ314は、コマンド処理部317に対して、アクセス処理部318によるディスク303へのアクセスを停止するように指示を出す。
- [0112] セクタ転送制御部313は、セクタ転送カウンタ314からセクタデータ351の出力の停止の指示を受けた場合、メッセージ伝達部316に対して、メッセージ362(この場合、エラーメッセージ)をホスト302に対して出力するように指示を出す。
- [0113] 一方、ホスト303の復号部322は、ドライブ装置301からインタフェースを介して暗号化されたセクタデータ351の供給をうける。復号部322は、ドライブ装置301から、セクタデータ351とは別の経路(詳細は図11を参照して後述する)で、乱数発生部315により発生された初期ベクトルIVも供給される。
- [0114] 復号部322は、認証処理部331から供給されるセッションキー $K_s$ と、ドライブ装置301から供給された初期ベクトルIVを用いて復号処理を実行し、セクタデータ361を生成する。
- [0115] ホスト302からは、コマンドパケット363が必要に応じて、ドライブ装置301に対して供給される。このコマンドパケット363は、例えば、ディスク303からデータの読み出しを指示するリードコマンド(Read command)、ディスク303へのデータの書き込みを指示するライトコマンド(Write command)、初期ベクトルIVの発行を指示するレポートキーコマンド(Report Key command)などがある。
- [0116] 図11を参照して、セクタデータ351が授受される経路と、その他のデータが授受される経路について説明する。PC driver391は、例えば、初期ベクトルIVの生成、暗

号化セクタデータの作成、転送セクタデータの作成などを制御するドライバーである。  
PC driver391からのデータは、Optical Disc driver392に渡される。

[0117] Optical Disc driver392は、光ディスク(Optical Disc)の読み出しや書き込みを制御するドライバーである。光ディスクがDVDなどの記録媒体である場合、その光ディスクに書き込まれているデータ(ファイル)は、UDF(Universal Data Format)に準拠したものとされている。よって、Optical Disc driver392により読み出された(制御された)データ(ファイル)は、UDF FS driver393の制御により、Optical Disc file reader394を介して、Video/Audio Playback function395に渡される。

[0118] Video/Audio Playback function395は、例えば、転送セクタデータの取得、初期ベクトルIVの取得、暗号化セクタデータの復号を制御する。

[0119] このように、セクタデータなどの映像や音声に関わるデータは、UDF FS driver393を介して授受されるが、その他の、例えば、初期ベクトルIVやその初期ベクトルIVを発行させるためのコマンドなどのデータは、UDF FS driver393を介さずに授受される。このUDF FS driver393を介さずに行われるデータの授受の経路は、Microsoft Windows(登録商標)においてはSCSI PASS Throughなどと称されている。

[0120] 図10において、ドライブ装置301とホスト302との間に図示されている線のうち、太線で示した経路が、UDF FS driver393を介してデータの授受が行われる経路(以下、適宜、UDF経路と称する)を示し、細線で示した経路が、その他のデータの授受が行われる経路(SCSI PASS Through、以下、適宜、パス経路と称する)を示すとする。

[0121] 図10に示したように、セクタ転送制御部313から復号部322への経路がUDF経路である。認証処理部311と認証処理部321との間で行われる認証処理に必要とされるデータの授受は、パス経路を介して行われる。また、メッセージ伝達部316から出力されるメッセージ362は、パス経路を介して授受される。また、初期ベクトルIVも、パス経路を介して授受される。

[0122] UDF FS driver393は、2048バイトのデータ、または、2048バイトの整数倍のデータ容量のデータを取り扱う。よって、UDF経路を介して授受されるデータは、2048バイトまたはその倍数のデータしか通すことができない。

[0123] これに対し、パス経路は、基本的にデータの容量にかかわらず授受することが可能

である。よって、16バイトで構成される初期ベクトルIVなどを授受をするのに適した経路である。

- [0124] 図10に示した構成のドライブ装置301の動作について、図12と図13のフローチャートを参照して説明する。ステップS31において、ドライブ装置301にディスク303が、挿入されたか否かが判断される。ステップS31において、ドライブ装置301にディスク303が挿入されたと判断された場合、ステップS32に処理が進められ、ホスト302において所定のアプリケーションが起動されたか否かが判断される。
- [0125] 所定のアプリケーションとは、ドライブ装置301に挿入されたディスク303からデータを読み出す、または、書き込むために必要とされるアプリケーションである。
- [0126] ステップS32において、ホスト302において所定のアプリケーションが起動されたと判断された場合、ステップS33に処理が進められる。ステップS33において、ドライブ装置301とホスト302との間で相互認証処理が実行され、セッションキーKsが、ドライブ装置301とホスト302で、それぞれ生成(共用)される。ステップS34において、セッションキーKsの生成が完了したか否かが判断される。セッションキーKsの生成が完了されるまで、ステップS33とステップS34の処理が繰り返される。
- [0127] そして、ステップS34において、セッションキーKsの生成が完了したと判断されると、ステップS35に処理が進められ、ドライブ装置301のセクタ転送カウンタ314のカウント値Nが、予め設定されているカウンタ値Nの最大値である値Nmaxに設定される(N=Nmaxに設定される)。
- [0128] このように、N=Nmaxに設定されると、セクタ転送カウンタ314の指示により、セクタ転送制御部313からホスト302へのデータの出力が許可されない状態に設定される。
- [0129] ステップS36において、ホスト302から初期ベクトルIVの転送要求があったか否かが判断される。この判断は、コマンド処理部317が、ホスト302側から、コマンドパケット363を受信したか否かを判断し、かつ、受信したコマンドパケット363が、初期ベクトルIVの転送要求を示すものであるか否かを判断することにより行われる。
- [0130] ステップS36において、初期ベクトルIVの転送要求があったと判断されるまで、ステップS36の処理が繰り返される。そして、ステップS36において、初期ベクトルIVの転



送要求があったと判断された場合、ステップ37に処理が進められ、初期ベクトルIVの生成が行われる。

- [0131] コマンド処理部317は、ホスト302からのコマンドパケット363を受信し、そのコマンドパケット363を解析することにより、初期ベクトルIVの転送要求であると判断すると、そのことを、乱数発生部315に知らせる。そのような知らせを受けた乱数発生部315は、ステップS37の処理として、初期ベクトルIVを生成する。
- [0132] 乱数発生部315は乱数を発生するが、その乱数が、そのまま初期ベクトルIVとされる。または、発生された乱数と所定の情報(例えば、初期ベクトルIVの転送要求を指示するコマンドパケット363に含まれる情報)などを用い、排他的論理和を算出するなどの処理が実行されることにより、初期ベクトルIVが発生されるようにしても良い。
- [0133] 乱数発生部315は、初期ベクトルIVを生成すると共に、セクタ転送カウンタ314に対して、カウンタ数Nを0に設定し直すように指示を出す。このような指示を受け取ったセクタ転送カウンタ314は、ステップS38の処理として、カウンタ値Nを0に設定し直す。このようにセクタ転送カウンタ314のカウンタ値Nが、0に設定されると、セクタ転送制御部313からのデータの出力が許可された状態に変更される。
- [0134] 乱数発生部315により生成された初期ベクトルIVは、ステップS39において、ホスト302に供給される。この初期ベクトルIVの供給(転送)は、パス経路を介して行われるため、例えば、初期ベクトルIVが16バイトで構成される場合であっても、その16バイトの初期ベクトルIVをドライブ装置301とホスト302側で授受することが可能である。
- [0135] ステップS33乃至S39の処理のうち、初期ベクトルIVの授受に関わる処理について、図14を参照して説明を加える。
- [0136] ホスト302は、ステップS101において、ドライブ装置301は、ステップS111において、それぞれ相互認証(Authentication)を行う。この相互認証が正常に行われた場合のみ、次のステップに処理が進められる。また、この相互認証の結果、ドライブ装置301の認証処理部311とホスト302の認証処理部321との、それぞれにおいてセッションキーKsが生成される(共有される)ことになる。
- [0137] ホスト302は、ステップS102において、コマンドパケット363を生成し、ドライブ装置301に対して出力する。ステップS102において生成され、出力されるコマンドパケッ

ト363は、REPORT KEY commandであり、このREPORT KEY commandは、ここでは、初期ベクトルIVの転送を要求するものであるとする。

- [0138] そのようなREPORT KEY commandを、ステップS112の処理として受信したドライブ装置301は、ステップS113において、初期ベクトルIVを生成する。生成された初期ベクトルIVは、ステップS114において、ドライブ装置301からホスト302に対して出力される。この出力される初期ベクトルIVは、そのままホスト302側に出力される。
- [0139] このようにしてドライブ装置301から出力された初期ベクトルIVを、ホスト303は、ステップS103において受信する。
- [0140] このように、ドライブ装置301からホスト302に転送される初期ベクトルIVを、暗号化などの処理を施さずに、そのまま転送されるようにしても良いが、暗号化が施された状態で転送されるようにしてももちろん良い。
- [0141] 初期ベクトルIVは、乱数発生部315により乱数を用いて発生されるため、ランダムに変化される値である。また、初期ベクトルIVは、セッションキーKsと異なり、秘匿する必要性は低いと考えられる。このようなことを考慮し、図14を参照して説明したように、転送される初期ベクトルIVは、そのまま転送されるようにしても良い。
- [0142] しかしながら、初期ベクトルIVは、予測不可能であることが好ましいという条件がある。その条件を満たすために、転送される初期ベクトルIVを暗号化し、より安全性を高めるようにしてももちろん良い。
- [0143] より安全性を高めて初期ベクトルIVが転送されるようにした場合、図15に示すように処理が行われる。ホスト302側で行われるステップS131乃至S133における処理は、基本的に、図14におけるステップS101乃至S103と同様に行われるが、ステップS103において受信される初期ベクトルIVは、暗号化されているため、受信された後に、復号という処理が実行される点が異なる。
- [0144] ドライブ装置301側で行われるステップS141乃至S144における処理も、基本的に、図14におけるステップS111乃至S114と同様であるが、ステップS143において、初期ベクトルIVが生成されたあと、その初期ベクトルIVが、セッションキーKsが用いられて暗号化され、その暗号化された初期ベクトルIV( $E[Ks, IV]$ )が、ステップS144における処理としてホスト302側に転送される点が異なる。

- [0145] このようにして、ホスト302側から初期ベクトルIVの転送要求があると、ドライブ装置301は、初期ベクトルIVを生成し、ホスト302側に転送する。もちろん、ドライブ装置301は、生成した初期ベクトルIVを、ホスト302側に転送するだけでなく、自己の暗号化部312(図10)にも供給する。
- [0146] 図12のフローチャートの処理の説明に戻り、ステップS39における初期ベクトルIVの転送の処理が終了されると、ステップS40(図13)に処理が進められる。ステップS40において、初期ベクトルIVの再発行要求があったか否かが判断される。ステップS40において、初期ベクトルIVの再発行要求があったと判断された場合、ステップS41乃至S43の処理が実行される。
- [0147] ステップS41乃至S43は、基本的に、ステップS37乃至ステップS38の処理と同様であるが、図16を参照して説明を加える。ホスト301は、ステップS161において、初期ベクトルIVの再発行要求をドライブ装置301に対して出す。この再発行要求は、コマンドパケット363が出力されることにより行われるが、このコマンドパケット363は、例えば、図14のステップS102において発行されるREPORT KEY commandと同じである。
- [0148] ドライブ装置301は、ステップS171において、REPORT KEY commandを受信すると、ステップS172において、初期ベクトルIVを再生成する。初期ベクトルIVの再生成は、図14のステップS113、または、図15のステップS143の処理と同様に行われる。そして、再生成された初期ベクトルIVは、ステップS173において、ホスト302側に転送される。この転送時に、初期ベクトルIVは、暗号化が施されて転送されるようにしても良いし、そのまま転送されるようにしても良い。
- [0149] 図13のフローチャートの説明に戻り、ステップS40において、初期ベクトルIVの再発行要求はないと判断された場合、または、ステップS43における処理として初期ベクトルIVの転送に関わる処理が終了した場合、ステップS44に処理が進められる。
- [0150] ステップS44において、セクタデータ351の転送要求があったか否かが判断される。この判断は、コマンド処理部317が、ホスト302側から、コマンドパケット363を受信したか否かを判断し、かつ、受信したコマンドパケット363が、セクタデータ351の転送を要求するものであるか否かを判断することにより行われる。

- [0151] ステップS44において、セクタデータ351の転送要求はないと判断された場合、ステップ40に処理が戻され、それ以降の処理が繰り返される。一方、ステップS44において、セクタデータ351の転送要求があったと判断された場合、ステップ45に処理が進められる。
- [0152] ステップS45において、セクタ転送カウンタ314のカウント値Nが、 $N > N_{\max}$ という関係を満たすか否かが判断される。ステップS45において、 $N > N_{\max}$ という関係は満たされていないと判断された場合、ステップS46に処理が進められる。 $N > N_{\max}$ という関係が満たされていない状態、すなわち、 $N < N_{\max}$ という関係を満たす状態のときには、セクタ転送制御部313からのデータの出力(ホスト302側へのデータの転送)が許可されている状態である。
- [0153] そこで、ステップS46においては、セクタ転送制御部313からホスト302側へのデータの転送が行われる。まず、コマンド処理部317の指示により、アクセス処理部318が、ディスク303からセクタデータ351の読み出しの制御を行う。アクセス処理部318の制御により、ディスク303から読み出されたセクタデータ351は、暗号化部312に供給される。
- [0154] 暗号化部312は、認証処理部311から供給されるセッションキーKsと、乱数発生部315から供給される初期ベクトルIVを用いて、セクタデータ351を暗号化する。暗号化されたセクタデータ351は、セクタ転送制御部313の制御により、ホスト302に転送される。この際、セクタデータ351が転送される経路は、UDF経路であり、そのデータ量は、2048バイト(または、2048の整数倍のバイト数)とされている。
- [0155] 暗号化部312からデータが出力されると、その情報は、セクタ転送カウンタ314に供給される。セクタ転送カウンタ314は、ステップS47において、自己が管理しているカウント値Nを、 $N+1$ の値に更新し、その更新された値を新たなカウント値Nと設定する。セクタ転送カウンタ314におけるカウント値Nの更新が終了されると、ステップS40に処理が戻され、それ以降の処理が繰り返される。
- [0156] このセクタデータ351の転送に関わる処理について、図17のタイミングチャートを参照して、説明を加える。ホスト302は、ステップS201において、リードコマンド(READ command)を発行する。リードコマンドは、ディスク303からセクタデータ351を指示す

る際に発行されるコマンドである。また、後述するように、ディスク303にデータを書き込む際にはライトコマンド(WRITE command)が発行される。

- [0157] 発行されるリードコマンドは、例えば、図18に示したデータ構成を有するコマンドパケット363の一種である。コマンドの詳細はINCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)” に記述がある。
- [0158] 図18に示したコマンドパケット363は、リードコマンドまたはライトコマンドの形式を示すものである。図18に示したコマンドパケット363内のデータのうち、以下の説明に必要な部分のデータについて説明を加える。
- [0159] “Operation Code”には、リードコマンドであるか、ライトコマンドであるかを示すデータが書き込まれる。よって、この部分に書き込まれているデータを参照することで、ホスト302からコマンドを受け取ったドライブ装置301は、リードコマンドであるか、ライトコマンドであるかを判別することが可能となっている。また、“Operation Code”は、1バイトのデータである。
- [0160] “Logical Block Address”には、コマンドパケット363がリードコマンドである場合には、読み出すべきアドレスの開始LBAが書き込まれ、コマンドパケット363がライトコマンドである場合には、書き込むべきアドレスの開始LBAが書き込まれている。また、“Logical Block Address”は、4バイトのデータである。
- [0161] “Transfer Length”には、コマンドパケット363がリードコマンドである場合には、読み出しセクタ数を指示するデータが書き込まれ、コマンドパケット363がライトコマンドである場合には、書き込みセクタ数を指示するデータが書き込まれる。また、“Transfer Length”は、4バイトのデータである。
- [0162] ステップS201において、ホスト302から発行されるコマンドパケット363は、“Operation Code”がリードコマンドを示す値が記載されているコマンドである。ここでは、その発行されるリードコマンドに含まれる“Transfer Length”は“N1”であるコマンドが発行されたとする。
- [0163] ステップS201における処理で発行されたリードコマンドは、ステップS231において、ドライブ装置301のコマンド処理部317に供給される。コマンド処理部317は、供給されたコマンドの“Operation Code”を参照し、リードコマンドであることを認識する。そ

して、“Logical Block Address”を参照し、データの読み出しを開始するアドレスを認識し、“Transfer Length”を参照して、この場合、“Transfer Length”=N3ということ認識する。

- [0164] コマンド処理部317は、認識結果を、アクセス処理部318に供給する。アクセス処理部318は、コマンド処理部317からの認識結果に基づき、ディスク303からのデータの読み出しを制御する。アクセス処理部318における処理としては、アドレスの変換処理などがある。
- [0165] アクセス処理部318は、LBA/PSN変換を行う。LBAは、Logical Block Addressの略であり、PSNは、Physical Sector Numberの略である。LBAは、論理的なアドレスを示し、例えば、リードコマンドに含まれ、ディスク303上の読み出すべきデータの物理媒体に依存せずにドライブ装置301とホスト302との間で共通的に扱うことを可能とする論理的なアドレスを示す。
- [0166] LBAに対し、PSNは、物理的なアドレスを示す。コマンドパケット363には、LBAが含まれるが、このLBAは、ディスク303上の論理的なアドレスを示し、実際の物理的なアドレスは示していないため、物理媒体から読み出した物理的なアドレスを示すPSNから共通に扱える論理的なアドレスへ変換するといった処理が、必要に応じ行われる。その変換処理を、アクセス処理部318は行う。
- [0167] なお、ディスク303上のユーザに開放された記録領域であるユーザデータエリア(不図示)の物理セクタに対して、例えば、ある物理セクタ番号の物理セクタを基準として、シーケンシャルな論理セクタ番号の論理セクタが、順次割り当てられる。変換方法の事例はINCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)”に記述がある。
- [0168] LBAがPSNに変換されると、ステップS232の処理として、その変換されたPSNが指し示すディスク303上の位置が検索される。この検索の結果、ピックアップ(不図示)がディスク303上の、読み出すべき位置に移動されるなどの処理が実行され、ディスク303からセクタデータ351が読み出される。読み出されたセクタデータ351は、暗号化部312に供給される。
- [0169] 暗号化部312には、認証処理部311からセッションキーKsが供給され、乱数発生

部315から初期ベクトルIVも供給される。暗号化部312は、供給されたセッションキーKsと初期ベクトルIVを用いてセクタデータ351を暗号化する。暗号化されたセクタデータ351(この場合、Encrypted Sector Data #1)は、ステップS232の処理として、セクタ転送制御部313の制御のもと、ホスト302の復号部322に対して出力される。

[0170] 復号部322は、供給されたEncrypted Sector Data #1を、認証処理部321から供給されるセッションキーKsと、ドライブ装置301の乱数発生部315から供給された初期ベクトルIVを用いて復号し、セクタデータ361を生成する。このようにして生成されたセクタデータ361は、図示されていないアプリケーションソフトウェアやディスプレイやスピーカに提供される。

[0171] このような処理がドライブ装置301とホスト302間で繰り返される。ドライブ装置301から、順次、Physical Sector Data が読み出される。すなわち、ディスク303側からは、ドライブ装置301の検索制御に応じて順次、連続的にセクタデータが読み出されドライブ装置301に供給される。

[0172] ドライブ装置301は、ステップS233乃至S240の各ステップの処理において、順次、読み出したセクタデータを暗号化し、ホスト302の要求(リードコマンドの発行)に応じてホスト302に供給する。

[0173] ドライブ装置301は、ホスト302に対してセクタデータを転送する際、セクタ転送カウンタ314により管理されているカウンタ値Nの更新処理なども行う。例えば、ステップS232の処理として、セクタデータ351が暗号化されてホスト302側に転送されると、セクタ転送カウンタ314のカウンタ値Nは、1だけ増加された値に更新される(ステップ47の処理)。よって、このようなカウンタ値Nの更新の処理が繰り返される(セクタデータが、順次、ホスト302側に転送されると)、カウンタ値Nの値が、閾値Nmaxよりも大きくなる( $N > N_{max}$ を満たす)ときがある。

[0174] 図17を参照するに、 $(N1 + N2) < N_{max} < (N1 + N2 + N3)$ と設定されていたとする。このような場合、ステップS240において、 $(N1 + N2 + 1)$ 番目のセクタデータが出力された後の時点(セクタ転送カウンタ314が管理するカウンタ値Nが、 $(N1 + N2 + 1)$ となった後の時点)で、継続的に、セクタデータがディスク303から読み出され、暗号化され、転送されという処理が繰り返されると、カウンタ値Nの値は、順次1つづ

増加されるので、 $N > N_{\max}$ という条件を満たすようになる。

- [0175]  $N > N_{\max}$ という条件が満たされると、すなわち、ステップS45(図13)において、YESと判断されると、ステップS48(図17においては、ステップS241)に処理が進められる。
- [0176] ステップ48(ステップS241)において、エラーメッセージ(Error Message)がドライブ装置301からホスト302側に出力される。ドライブ装置301のセクタ転送カウンタ314は、自己がカウントしているカウンタ値Nが、閾値 $N_{\max}$ よりも大きくなったと判断したとき、セクタ転送制御部313に対して、暗号化部312から供給されるデータをホスト301側に出力しないように指示を出す。
- [0177] セクタ転送制御部313は、セクタ転送カウンタ314から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部316に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部316は、セクタ転送制御部313から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト302に対して送信する。このエラーメッセージは、ホスト302に、指示されたデータの供給はできないということを認識させるためのメッセージである。
- [0178] このようなメッセージが出力されると、ドライブ装置301側からはデータが出力されない状態とされる。換言すれば、ドライブ装置301側で、認証処理が正常に行われた結果、データの出力が許可された状態であっても、その状態が解除され、許可されない状態に変更される。
- [0179] このように、本実施の形態によれば、一度設定されたデータ出力の許可という状況を変更することが可能である。よって、エラーメッセージが出力された後、ホスト302から、ディスク303からのデータの読み出しが指示されても、その指示に対応して、データが読み出されることはない。
- [0180] エラーメッセージが出力されると、ドライブ装置301からホスト302へのデータの出力が停止される。このようなデータの出力が停止されてしまような状況が発生しないようにするためには、ホスト302側で、初期ベクトルIVの発行要求が、所定のタイミングでドライブ装置301に対して出されればよい。
- [0181] すなわち、初期ベクトルIVの発行が要求されれば(例えば、ステップS40(図13))、



セクタ転送カウンタ314のカウント値Nが0にリセットされる(ステップS42)。その結果、 $N > N_{\max}$ という条件が満たされることを回避できるため、エラーメッセージが出力されるような状況が発生する(ステップS48)ようなことを回避することができる。

[0182] ホスト302は、定期的に初期ベクトルIVの発行の要求を出す。定期的とは、例えば、初期ベクトルIVの発行を要求した後、転送を指示したデータ量の累計が所定のデータ量(例えば、16Mbyte(8K Sector))を超える毎に要求されるということである。または、初期ベクトルIVの発行を要求した後、所定の時間が経過する毎に要求されるということである。

[0183] いずれにしても、ホスト302は、所定のタイミングで、初期ベクトルIVの発行の要求を出す。よって、正常に(正当に)処理が実行されている間、ドライブ装置301側では、ステップS41乃至S43の処理が定期的に行われることになり、定期的にセクタ転送カウンタ314のカウント値Nが0に設定されることになる。

[0184] このようにすることで、少なくとも以下のような問題を解決することができる。

ドライブ装置301とホスト302との間で一旦、相互認証が成功したら、ドライブ装置301は、相手(ホスト302において起動されているアプリケーションなど)が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題。

バスを第3者が観測し、保護されたデータを横取りして解読し平文化してしまうといった問題(不正に利用されてしまうという問題)。

[0185] このような問題を解決するために、上述したように、まず、保護されたデータ(ディスク303に記録されているセクタデータ351)をドライブ装置301からホスト302にバス転送する際、その保護されたデータをセッションキーKsで暗号化してから転送するようにした。このことにより、仮に、バスを第3者が観測し、保護されたデータを横取りしたとしても、そのデータを解読し平文化することを困難にすることが可能となる。

[0186] そして、データを暗号化する際、初期ベクトルIVを適用するようにした。またその初期ベクトルIVは、乱数を用いてランダムに変更されるようにした。このようにすることで、仮に、第3者が何らかの方法で、保護されたデータを横取りしたとしても、そのデータを解読し平文化することをより困難にすることが可能となる。

- [0187] また、初期ベクトルIVが変更されるようすることで、平文データが特別なデータであることを特定させることを困難にすることが可能となる。このことは、データのすり替えや、データの改竄など、不正な行為を防止できることを意味する。さらに、初期ベクトルIVを適宜更新させることで、大量のデータを単一の鍵で暗号化した場合に、暗号鍵(セッションキーKs)が予測されやすくなるといった問題を解決することが可能となる。
- [0188] また、上述したように、本実施の形態によれば、ホスト302側から適切に初期ベクトルIVの更新が指示されなければ、データの供給が停止されるため、ドライブ装置301とホスト302との間で一旦、相互認証が成功したら、ドライブ装置301は、相手(ホスト302において起動されているアプリケーションなど)が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題を解決することができる。
- [0189] すなわち、正当なドライブ装置301は、正当なホスト302にのみ、保護されたデータを転送するように制御することが可能となる。
- [0190] 上述した実施の形態においては、初期ベクトルIVが更新されるとしたが、暗号化に用いられるセッションキーKs自体が更新されるようにしても良い。換言すれば、ホスト302からは、初期ベクトルIVの再発行の指示が出されるのではなく、セッションキーKsの再発行の処理が出されるようにしても良い。
- [0191] しかしながら、セッションキーKsは、相互認証が正常に終了されなければ生成されないため、セッションキーKsの更新に係る処理時間や処理能力を考慮すると、初期ベクトルIVの方を更新する方が好ましいと考えられる。
- [0192] 上述した実施の形態においては、ディスク303からデータを読み出す(再生)の場合を例に挙げて説明したが、本発明はデータの再生にのみ適用範囲が限定されるわけではない。すなわち、本発明を、ディスク303へのデータの書き込み(記録)に適用することも可能である。
- [0193] 図19は、本発明を記録装置に適用した場合のシステム構成例を示す図である。
- [0194] 図19に示し記録装置のドライブ装置401は、ホスト402から供給されるデータを、セットされているディスク303に記録する。ドライブ装置401は、認証処理部411、復号

部412、セクタ転送制御部413、セクタ転送カウンタ414、乱数発生部415、メッセージ伝達部416、コマンド処理部417、および、アクセス処理部418を含む構成とされている。

[0195] ホスト402は、認証処理部421、暗号化部422を含む構成とされている。

[0196] 図19に示した記録装置の構成は、図10に示した再生装置の構成と同様な部分が多いので、その詳細な説明は省略し、異なる部分についてのみ説明を加える。

[0197] 図19に示した記録装置は、ディスク403にセクタデータを451を記録する。この記録されるセクタデータ451は、ホスト402側から供給されるセクタデータ461である。ホスト402の暗号化部422は、図示されていない記録媒体またはハードディスクドライブなどから読み出されたセクタデータ461を、認証処理部421から供給されるセッションキーKsを用いて暗号化する。

[0198] 暗号化部422により暗号化されたセクタデータ461は、ドライブ装置401のセクタ転送制御部413に供給される。セクタ転送制御部413は、供給されたセクタデータ461を、復号部412に供給する。復号部412は、供給されたセクタデータ461を、認証処理部411から供給されるセッションキーKsを用いて復号する。復号されたセクタデータ461は、セクタデータ451として、アクセス処理部418の制御のもと、ディスク403に記録される。

[0199] セクタ転送カウンタ414は、セクタ転送制御部413から出力され、復号部412に供給されたセクタ数をカウントする。その他の部分に関しては、図10に示した再生装置の対応する部分と、基本的に同様な構成であり、その動作も同様である。

[0200] 図19に示した記録装置のドライブ装置401は、既に図12、図13のフローチャートを参照して説明した処理と、基本的に同様な処理を実行するため、詳細な説明は省略する。ここでは、再度、図12、図13のフローチャートを参照し、異なる処理のみに説明を加える。

[0201] ドライブ装置401は、ステップS44において、セクタデータの記録の要求があったか否かを判断する。この判断は、コマンド処理部417が、ホスト402側から、コマンドパケット463を受信したか否かを判断し、かつ、受信したコマンドパケット463が、セクタデータ461の書き込みを要求するもの（すなわち、ライトコマンド）であるか否かを判断

することにより行われる。

- [0202] また、ステップS46においては、暗号化されたセクタデータ461が供給されるため、復号部412における復号処理が行われ、その復号されたセクタデータ461(451)がディスク403に書き込まれる処理が実行される。その他の処理については、基本的に同様であり、ホスト402から定期的に初期ベクトルIVの発行要求が出されなければ、ドライブ装置401側における書き込みの処理が停止される(ホスト403からのデータの出力が停止される)ように制御される。
- [0203] よって、ホスト402側で管理している保護されたデータが、不正に出力されること、そして、ディスク403に書き込まれてしまふことを防ぐことが可能となる。
- [0204] 図20のタイミングチャートを参照して、図19に示した記録装置における、データの記録に関わる処理について説明を加えるが、基本的な処理は、図17に示したタイミングチャートと同様であるので、その詳細な説明は省略する。異なる処理としては、ステップS301において、ホスト402から、データの書き込みを指示するライトコマンド(WRITE command)が送信される。
- [0205] また、ステップS302において、ホスト402の暗号化部422は、セクタデータ461をセッションキーKsを用いて暗号化し、その暗号化したデータ(Encrypted Sector Data #1)を、ドライブ装置401に対して送信する。ドライブ装置401のセクタ転送制御部423は、供給されたEncrypted Sector Data #1を、復号部412に供給する。
- [0206] 復号部412は、認証処理部411から供給されるセッションキーKsと、乱数発生部415から供給された初期ベクトルIVを用いて復号し、セクタデータ451を生成する。このようにして生成されたセクタデータ451は、アクセス処理部418の制御に基づき、ディスク403に書き込まれる。
- [0207] このような処理が行われると共に、セクタ転送カウンタ414は、セクタ転送制御部413から出力されたセクタ数をカウントする。そして、そのカウントされているカウンタ値Nが、Nmax以上になったか否かの判断を行う。カウンタ値Nが大きくなると、すなわち、セクタデータが、順次、セクタ転送制御部413から出力されると、カウンタ値Nの値が、閾値Nmaxよりも大きくなる( $N > N_{max}$ を満たす)ときがある。
- [0208] 図20を参照するに、 $(N1 + N2) < N_{max} < (N1 + N2 + N3)$ と設定されていたとす

る。このような場合、ステップS340において、 $(N1 + N2 + 1)$ 番目のセクタデータが受信された後の時点(セクタ転送カウンタ414が管理するカウンタ値Nが、 $(N1 + N2 + 1)$ となった後の時点)で、継続的に、セクタデータがディスク403に書き込まれるという処理が繰り返されると、カウンタ値Nの値は、順次1つづ増加されるので、 $N > N_{max}$ という条件を満たすようになる。

[0209]  $N > N_{max}$ という条件が満たされると、すなわち、ステップS45(図13)において、YESと判断されると、ステップS48(図20においては、ステップS341)に処理が進められる。

[0210] ステップ48(ステップS341)において、エラーメッセージ(Error Message)がドライブ装置401からホスト402側に出力される。ドライブ装置401のセクタ転送カウンタ414は、自己がカウントしているカウンタ値Nが、閾値 $N_{max}$ よりも大きくなったと判断したとき、セクタ転送制御部413に対して、復号部412にデータを出力しないように指示を出す。

[0211] セクタ転送制御部413は、セクタ転送カウンタ414から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部416に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部416は、セクタ転送制御部413から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト402に対して送信する。このエラーメッセージは、ホスト402に、指示されたデータの書き込みはできないということを認識させるためのメッセージである。

[0212] このようなメッセージが出力されると、ドライブ装置401側からはデータが入力されない状態とされる。また、エラーメッセージを受け取ったホスト402は、データを出力しない状態とされる。

[0213] このように処理が行われることで、既に説明した再生装置の場合と同様の効果を望むことが可能である。

[0214] このように、本発明を適用することにより、ドライブ装置とホストとの間で行われるデータの授受に関し、セキュリティを向上させることが可能となる。

[0215] なお、上述した実施の形態においては、再生装置(図10)と記録装置(図19)をそれぞれ別な構成として図示および説明したが、再生装置と記録装置を同一の装置内

に納めることも可能である。同一の装置内に納めるようにした場合、再生装置内と記録装置内において同一の処理を実行する、例えば、乱数発生部315(415)などは、再生装置と記録装置で共用される構成としても、もちろん良い。

[0216] なお、上述した実施の形態においては、暗号化および復号の方式として、CBC方式を例に挙げて説明したが、本発明は、CBC方式にのみ適用できることを示すものではない。例えば、CFB(Cipher Feed Back)方式、OFB(Output Feed Block)方式などに対しても本発明を適用することはできる。

[実施例2]

[0217] 実施例1においては、ドライブ装置301(401)側で初期ベクトルIVを生成する場合を例にあげて説明したが、実施例2とし、ホスト側で初期ベクトルIVを生成する場合について説明する。

[0218] 図21は、実施例2におけるシステムの構成を示す図である。ドライブ装置501は、認証処理部511、復号部512、入力制御部513、セクタ転送カウンタ514、リセット処理部515、メッセージ伝達部516、コマンド処理部517、および、アクセス処理部518を含む構成とされている。

[0219] ホスト502は、認証処理部521、暗号化部522、セクタ転送カウンタ523、乱数発生部524、および、スイッチ525を含む構成とされている。

[0220] 図21に示したシステムにおいては、ホスト502からドライブ装置501に対して、暗号化された状態のセクタデータ561が供給され、そのセクタデータ561が、復号された後に、セクタデータ551としてディスク503に書き込まれる。

[0221] ドライブ装置501の認証処理部511とホスト502の認証処理部521により、相互認証に関わる処理が実行される。

[0222] ホスト502の暗号化部522には、ディスク503に書き込まれるセクタデータ561と、認証処理部511からセッションキーKsが供給される。また、暗号化部522には、乱数発生部524により発生された乱数が、初期ベクトルIVとして供給される。暗号化部522は、供給されたセクタデータ561をセッションキーKsと初期ベクトルIVを用いて暗号化し、ドライブ装置501に送信する。

[0223] ドライブ装置501の入力制御部513は、ホスト502から、暗号化されたセクタデータ

561を入力した場合、復号部512に転送する。復号部512には、ホスト502から、セクタデータ561とは別の経路で、乱数発生部524により発生された初期ベクトルIVも供給される。

- [0224] 復号部512は、認証処理部511から供給されるセッションキー $K_s$ と、ホスト502から供給される初期ベクトルIVを用いて復号処理を実行し、セクタデータ551(セクタデータ561と同一のデータ)を生成する。生成されたセクタデータ551は、ディスク503に書き込まれる。この書き込みは、アクセス処理部518の制御のもと行われる。
- [0225] ホスト502は、セクタデータ561を出力する際、セクタ転送カウンタ523により、転送する(転送した)セクタ数をカウントするように構成されている。そして、そのカウント数に応じ、スイッチ525を切り換えるように構成されている。詳細は後述するが、カウント数(以下、適宜、カウント値 $N$ とする)が、所定の数(以下、適宜、閾値 $N_{max}$ とする)に達する前の時点で、センドキーコマンド563により、初期ベクトルIVを転送するように構成されている。
- [0226] 同様に、ドライブ装置501側にも、セクタ転送カウンタ514が設けられている。セクタ転送カウンタ514は、入力制御部513から復号部512に供給されたセクタ数をカウントしている。セクタ転送カウンタ514は、カウント数(以下、適宜、カウント値 $M$ とする)が所定の数(以下、適宜、閾値 $M_{max}$ とする)に達した場合、入力制御部513にセクタデータを入力しないように指示を出すとともに、メッセージ伝達部516に対してメッセージの伝達を指示する。
- [0227] なお、ホスト502のセクタ転送カウンタ523に設定されている閾値 $N_{max}$ は、ドライブ装置514のセクタ転送カウンタ514に設定されている閾値 $M_{max}$ よりも小さい値とされている( $N_{max} < M_{max}$ という条件を満たす値とされている)。
- [0228] また、ここでは、セクタ転送カウンタ514は、カウント値 $M$ が閾値 $M_{max}$ に達した場合、入力制御部513にセクタデータを入力しないように指示を出すとして説明を続けるが、入力制御部513に、入力されたセクタデータを復号部512に転送しないように指示を出すようにしても良い。
- [0229] セクタ転送カウンタ514のカウント値 $M$ をリセットする(0にする)ために、リセット処理部515が設けられている。リセット処理部515に対する指示は、コマンド処理部517

により出される。

- [0230] このような構成を有するシステムにより行われる処理について説明する。まず、図22のタイミングチャートを参照して、初期ベクトルIVに係る処理について説明する。ホスト502は、ステップS501において、ドライブ装置501は、ステップS521において、それぞれ相互認証(Authentication)を行う。この相互認証が正常に行われた場合のみ、次のステップに処理が進められる。また、この相互認証の結果、ドライブ装置501の認証処理部511とホスト502の認証処理部521との、それぞれにおいてセッションキーKsが生成される(共有される)ことになる。
- [0231] ホスト502は、ステップS502において、 SEND キー コマンド (SEND KEY command) 563を生成し、ドライブ装置501に対して出力する。ステップS502において生成され、出力される SEND キー コマンド 563は、初期ベクトルIVの転送するためのものである。
- [0232] ステップS503において、初期ベクトルIVが生成され、転送される。この初期ベクトルIVは、 SEND キー コマンド 563により転送される。ドライブ装置501は、ステップS522, S523により、 SEND キー コマンド 563および初期ベクトルIVを受信する。コマンド処理部517は、受信した SEND キー コマンド 563を、リセット処理部515に供給する。
- [0233] リセット処理部515は、 SEND キー コマンド 563が供給された場合、セクタ転送カウンタ514に対して、カウント値Mをリセットするように(0に戻すように)指示を出す。また、 SEND キー コマンド 563に含まれる初期ベクトルIVは、復号部512に供給される。
- [0234] このようにして、ドライブ装置501とホスト502の両方で、共通のセッションキーKsと初期ベクトルIVが共用される。共通のセッションキーKsと初期ベクトルIVが共用された後の処理について、図23のタイミングチャートを参照して説明する。
- [0235] ステップS551において、ホスト502から、セクタデータの書き込みを指示するライトコマンド(WRITE command)が送信される。また、ステップS552において、ホスト502の暗号化部522は、セクタデータ561をセッションキーKsと初期ベクトルIVを用いて暗号化し、その暗号化したデータ(Bus-Encrypted Sector Data)を、ドライブ装置501に対して送信する。ドライブ装置501の入力制御部513は、供給された Bus-Encrypted Sector Dataを、復号部512に供給する。
- [0236] 復号部512は、認証処理部511から供給されるセッションキーKsと、乱数発生部52



4により発生され、供給された初期ベクトルIVを用いて復号し、セクタデータ551を生成する。このようにして生成されたセクタデータ551は、アクセス処理部518の制御に基づき、ディスク503に書き込まれる。

[0237] このような処理が行われると共に、ホスト502側のセクタ転送カウンタ523は、送信されたセクタ数をカウントする。そして、そのカウントされているカウンタ値Nが、 $N_{\max}$ 以上になったか否かの判断を行う。カウンタ値Nが大きくなると、すなわち、セクタデータが、順次、送信されると、カウンタ値Nの値が、閾値 $N_{\max}$ よりも大きくなる( $N > N_{\max}$ を満たす)ときがある。

[0238] そのような状況になると、ホスト502からは、センドキーコマンド563が送信される。図23のタイミングチャートにおいては、ステップS555のタイミングでセンドキーコマンド563が送信されている。

[0239] ホスト502から送信されたセンドキーコマンド563は、ステップS585においてドライブ装置501に受信される。ドライブ装置501のセクタ転送カウンタ514は、センドキーコマンド563が受信されたことによりリセットされる。よって、ホスト502から適切なタイミングでセンドキーコマンド563が出力されている間は、セクタ転送カウンタ514によるカウント値Mが閾値 $M_{\max}$ 以上になることはないため、入力制御部513によりデータの inputs が拒否されるような状況が発生するようなことがないため、ディスク503へのセクタデータの書き込みは継続的に行われることになる。

[0240] 次に、ドライブ装置501とホスト502の、それぞれの処理について説明を加える。図24と図25のフローチャートを参照して、ホスト502側の処理について説明する。ホスト502は、ステップS601において、所定のアプリケーションが起動されているか否かを判断する。所定のアプリケーションとは、ここでは、ドライブ装置501に挿入されたディスク503に対してデータを書き込むために必要とされるアプリケーションである。

[0241] ステップS601において、アプリケーションは起動されていると判断された場合、ステップS602において、ドライブ装置501にディスク503が、挿入されているか否かが判断される。ステップS602において、ドライブ装置501にディスク503が挿入されていると判断された場合、ステップS503に処理が進められ、ドライブ装置501とホスト502

との間で相互認証処理が実行され、セッションキーKsが、ドライブ装置501とホスト502で、それぞれ生成(共用)される。

- [0242] ステップS604において、セッションキーKsの生成が完了したか否かが判断される。セッションキーKsの生成が完了されるまで、ステップS603とステップS604の処理が繰り返される。
- [0243] そして、ステップS604において、セッションキーKsの生成が完了したと判断されると、ステップS605に処理が進められ、初期ベクトルIVが生成される。そして、ステップS606において、センドキーコマンド563が生成される。このようにして生成されたセンドキーコマンド563を用いて、初期ベクトルIVが、ステップS607の処理としてドライブ装置501側に送信される。
- [0244] ステップS608において、セクタ転送カウンタ523のカウント値Nが0にセットされる。ステップS609(図25)において、ライトコマンド(WRITE command)を送信するか否かが判断される。ライトコマンドではなく他のコマンドを送信すると判断された場合、ステップS610において、他のコマンドに対する処理が実行される。
- [0245] 一方、ステップS609において、ライトコマンドを送信すると判断された場合、ステップS611において、セクタ転送カウンタ523によりカウントされているカウント値Nが、 $N + L$ に更新される。このLは、ライトコマンドに含まれるTransfer Lengthの部分に書き込まれている数値である。このTransfer Lengthは、上述したように書き込みセクタ数を指示するデータであるため、Lが示す値は、その時点に送信されるセクタデータ数に対応していることになる。
- [0246] ステップS612において、セクタ転送カウンタ523によりカウントされているカウント値Nが、閾値 $N_{max}$ よりも大きくなったか否か( $N > N_{max}$ の条件を満たすか否か)が判断される。ステップS612において、 $N > N_{max}$ の条件を満たすと判断された場合、ステップS613に処理が進められる。 $N > N_{max}$ の条件を満たす状況とは、ここでは、センドキーコマンド563や初期ベクトルIVを送信する(更新する)タイミングであることを示している。
- [0247] ステップS613乃至S616の処理は、ステップS606乃至S608の処理と同様である。すなわち、センドキーコマンド563や初期ベクトルIVが新たに生成され、ドライブ装

置501側に送信される処理である。

- [0248] 一方、ステップS612において、 $N > N_{\max}$ の条件を満たさないと判断された場合、ステップS617に処理が進められ、ライトコマンドが生成され、送信される。そして、ステップS618において、セクタデータ561が、暗号化部522により暗号化され、その暗号化されたセクタデータ561が、ドライブ装置501側に送信される。
- [0249] このような処理が、ホスト502側で行われる一方で、ドライブ装置501側では、図26、図27に示すフローチャートの処理が実行される。
- [0250] ドライブ装置501は、ステップS631において、ディスク503が挿入されているか否かを判断する。ステップS631において、ドライブ装置501にディスク503が挿入されていると判断された場合、ステップS632に処理が進められる。ステップS632において、ホスト502側で所定のアプリケーションが起動されているか否かが判断される。
- [0251] ステップS632において、アプリケーションは起動されていると判断された場合、ステップS633において、ドライブ装置501とホスト502との間で相互認証処理が実行され、セッションキーKsが、ドライブ装置501とホスト502で、それぞれ生成(共用)される。
- [0252] ステップS634において、セッションキーKsの生成が完了したか否かが判断される。セッションキーKsの生成が完了されるまで、ステップS633とステップS634の処理が繰り返される。そして、ステップS634において、セッションキーKsの生成が完了したと判断されると、ステップS635に処理が進められる。
- [0253] ステップS635において、セクタ転送カウンタ514のカウンタ値Mが閾値Mmaxに設定される。このように、 $M = M_{\max}$ に設定されると、セクタ転送カウンタ514の指示により、入力制御部513でホスト502からのデータの入力が許可されない状態に設定される。
- [0254] ステップS636(図27)において、センドキーコマンド(SEND KEY command) 563を受信したか否かが判断され、受信したと判断された場合、ステップS637に処理が進められる。ステップS637において、センドキーコマンド563により送信されてきた初期ベクトルIVが受信される。センドキーコマンド563が受信されることで、リセット処理部515から、セクタ転送カウンタ514に対して、カウンタ数Mを0にリセットするように指示

が出される。

- [0255] このような指示を受け取ったセクタ転送カウンタ514は、ステップS638の処理として、カウンタ値Mを0にリセットする。このようにセクタ転送カウンタ514のカウンタ値Mが、0に設定される(閾値Mmax以下の状態にされる)ことにより、入力制御部613へのデータの入力が許可された状態にされる。
- [0256] ステップS639において、初期ベクトルIVが、復号部512に供給される。ステップS640において、ライトコマンド564を受信したか否かが判断され、受信していないと判断されると、ステップS636に戻り、それ以降の処理が繰り返される。一方、ステップS640において、ライトコマンド564を受信したと判断した場合、ステップS641に処理が進められる。
- [0257] ステップS641において、セクタ転送カウンタ514のカウンタ値MにTransfer Lengthの値Lを加算した値(M+L)が、閾値Mmax以上であるか否か(M+L>Mmaxという条件を満たすか否か)が判断される。ステップS641において、M+L>Mmaxという条件は満たされていないと判断された場合、ステップS642に処理が進められ、カウンタ値MがM+Lに更新される。M+L>Mmaxという条件が満たされていない状況とは、入力制御部513においてデータの入力が許可された状態を示す。
- [0258] ステップS643において、暗号化されているセクタデータ561が受信される。そして、受信されたセクタデータ561は、復号部512において復号され、セクタデータ551として、ディスク503に書き込まれる。
- [0259] 一方、ステップS641において、M+L>Mmaxという条件を満たすと判断された場合、ステップS644に処理が進められる。M+L>Mmaxという条件が満たされる状態になると、セクタ転送カウンタ514から入力制御部513に対してセクタデータの入力の停止が指示されるとともに、メッセージ伝達部516に対してメッセージの送信が指示される。
- [0260] メッセージ伝達部516から送信されるメッセージは、セクタデータの入力を許可しない(従って、ディスク503へのセクタデータの書き込みを許可しない)ということをホスト502に認識させるためのエラーメッセージである。ステップS644において、エラーメッセージが送信された後、ステップS636に処理が戻され、それ以降の処理が繰り返さ

れる。

- [0261] このようなエラーメッセージが出されることにより、ホスト502がドライブ装置501の状態を認識し、センドキーコマンドを発行し、初期ベクトルIVを供給すれば、すなわち、ステップS636において、センドキーコマンドを受信したと判断されれば、ステップS637以降に処理が進められるので、再度、セクタデータの入力が許可された状態に設定し直される。
- [0262] このように、ホスト502側で、初期ベクトルIVを生成し、また、その初期ベクトルIVの有効期間(寿命)を管理できるようにすることで、ドライブ装置とホストとの間で行われるデータの授受に関し、セキュリティを向上させることが可能となる。
- [0263] また、実施例2のようにした場合においても、実施例1の場合と同様な効果を得ることが可能である。
- [0264] 上述した一連の処理は、それぞれの機能を有するハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。
- [0265] 記録媒体は、その記録媒体を扱うパーソナルコンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク(フレキシブルディスクを含む)、光ディスク(CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク(MD(Mini-Disc)(登録商標)を含む)、若しくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記憶されているROMやハードディスクなどで構成される。
- [0266] なお、本明細書において、媒体により提供されるプログラムを記述するステップは、記載された順序に従って、時系列的に行われる処理は勿論、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。
- [0267] また、本明細書において、システムとは、複数の装置により構成される装置全体を

表すものである。

### 請求の範囲

- [1] データの転送を制御する転送制御手段と、  
前記転送制御手段が前記データの転送を制御した回数をカウントするカウント手段と、前記カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断手段と、  
前記第1の判断手段により前記回数が前記閾値以上になったと判断された場合、前記転送制御手段に、前記データの転送を停止するように指示を出す第1の指示手段と、  
前記転送制御手段により転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、  
前記転送制御手段により転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第2の判断手段と、  
前記第2の判断手段により前記初期ベクトルの供給が指示されたと判断された場合、前記生成手段に前記初期ベクトルの生成を指示するとともに、前記カウンタ手段によりカウントされている前記回数をリセットするように指示を出す第2の指示手段とを備えることを特徴とする情報処理装置。
- [2] 前記第1の指示手段による指示が出された場合、前記他の装置に対して前記データの転送が停止されたことを示すメッセージを出力する出力手段をさらに備えることを特徴とする請求項1に記載の情報処理装置。
- [3] データの転送を制御する転送制御ステップと、  
前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、  
前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、  
前記第1の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第1の指示ステップと、  
前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号

に用いられる初期ベクトルを生成する生成ステップと、

前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと

、  
前記第2の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第2の指示ステップと

を含むことを特徴とする情報処理方法。

[4] データの転送を制御する転送制御ステップと、

前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、

前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、

前記第1の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第1の指示ステップと、

前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、

前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと

、  
前記第2の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第2の指示ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

[5] データの転送を制御する転送制御ステップと、



前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、

前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、

前記第1の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第1の指示ステップと、

前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、

前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと

、  
前記第2の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第2の指示ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体

図1

[図1]

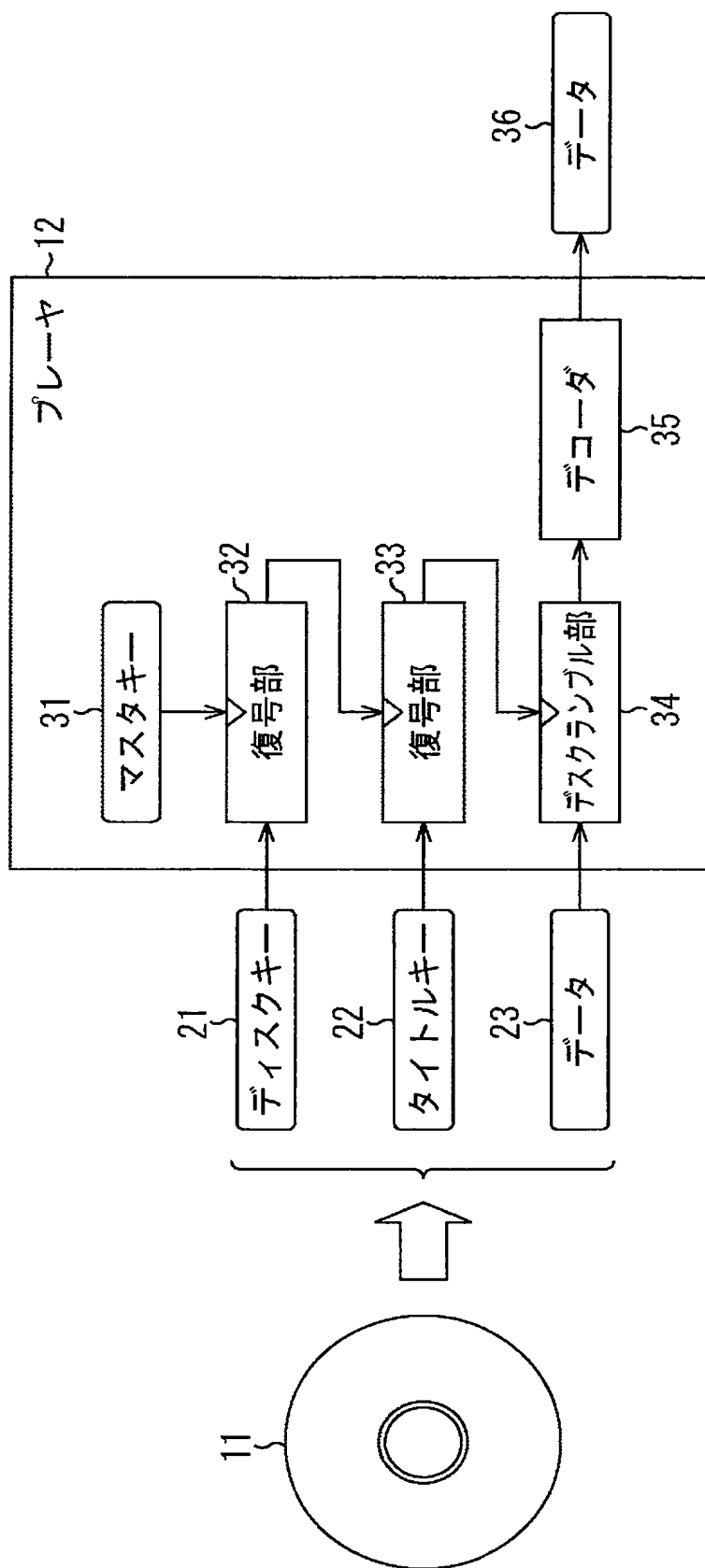
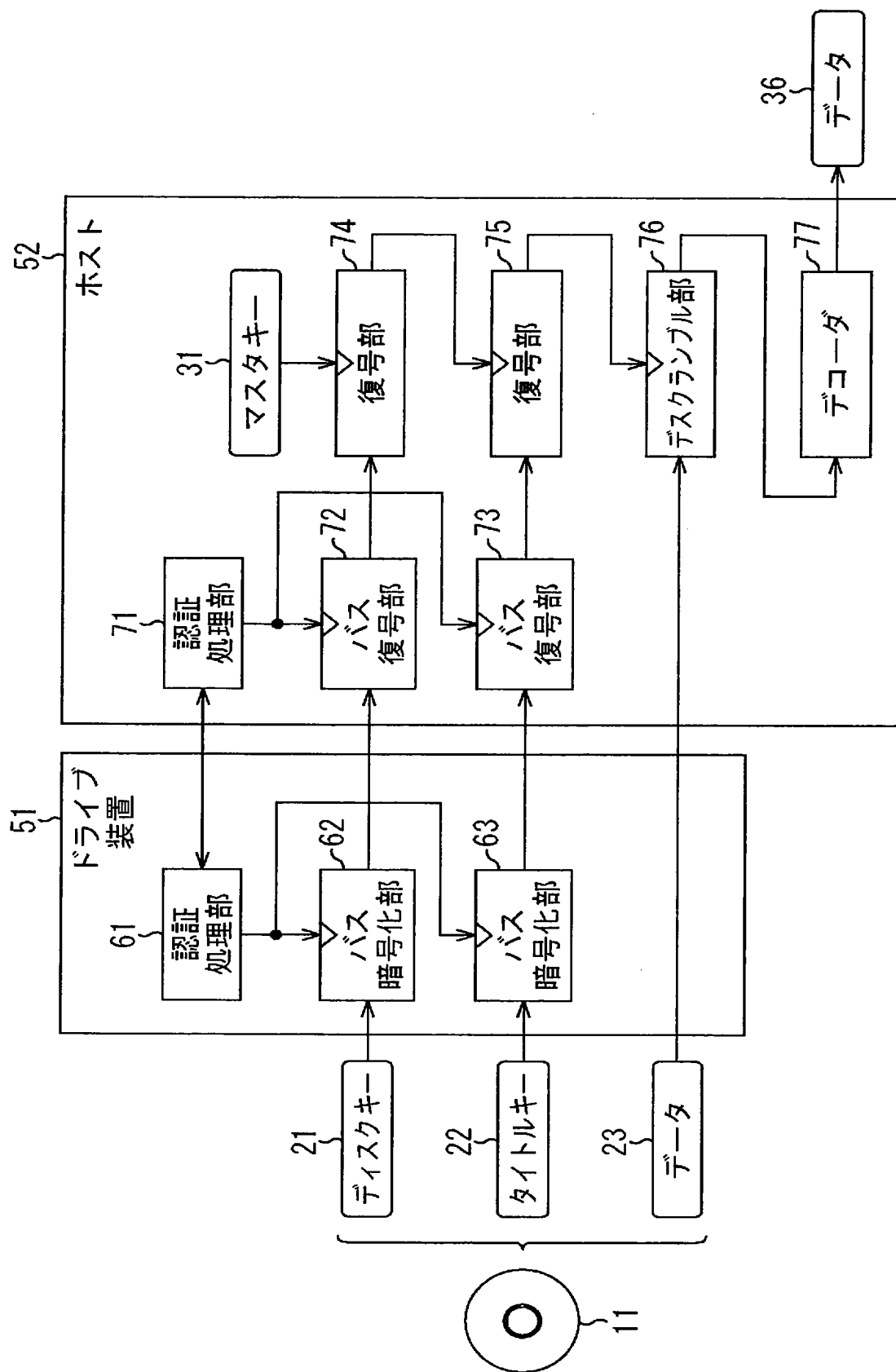


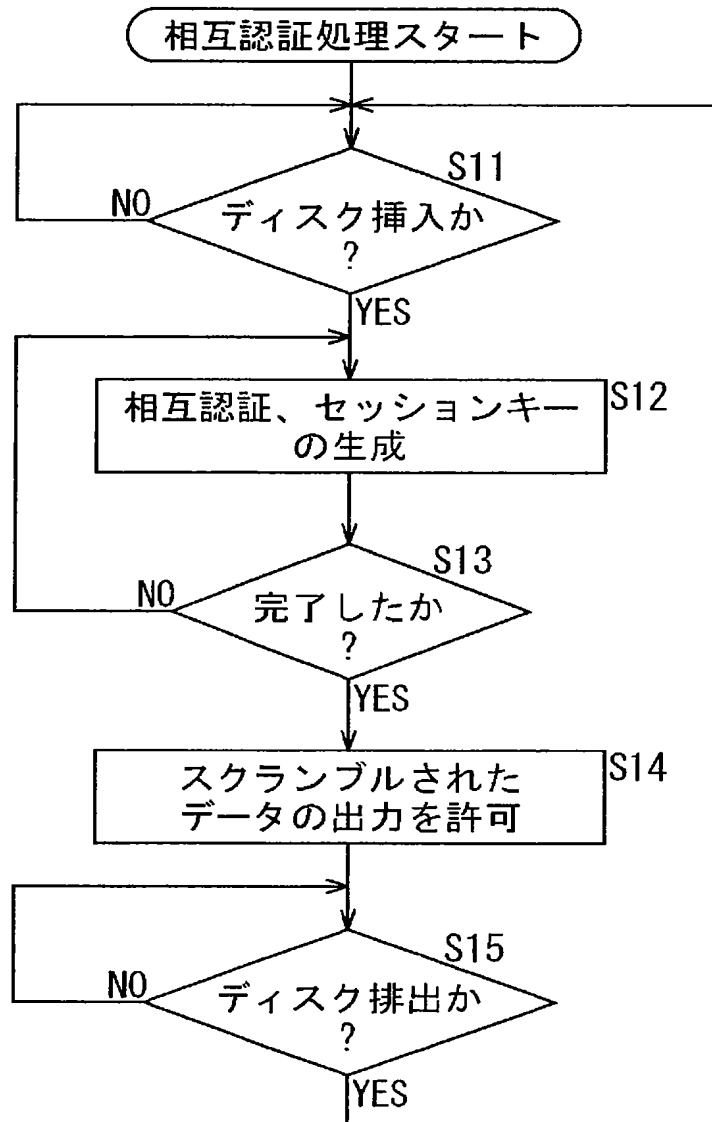
図2

図2



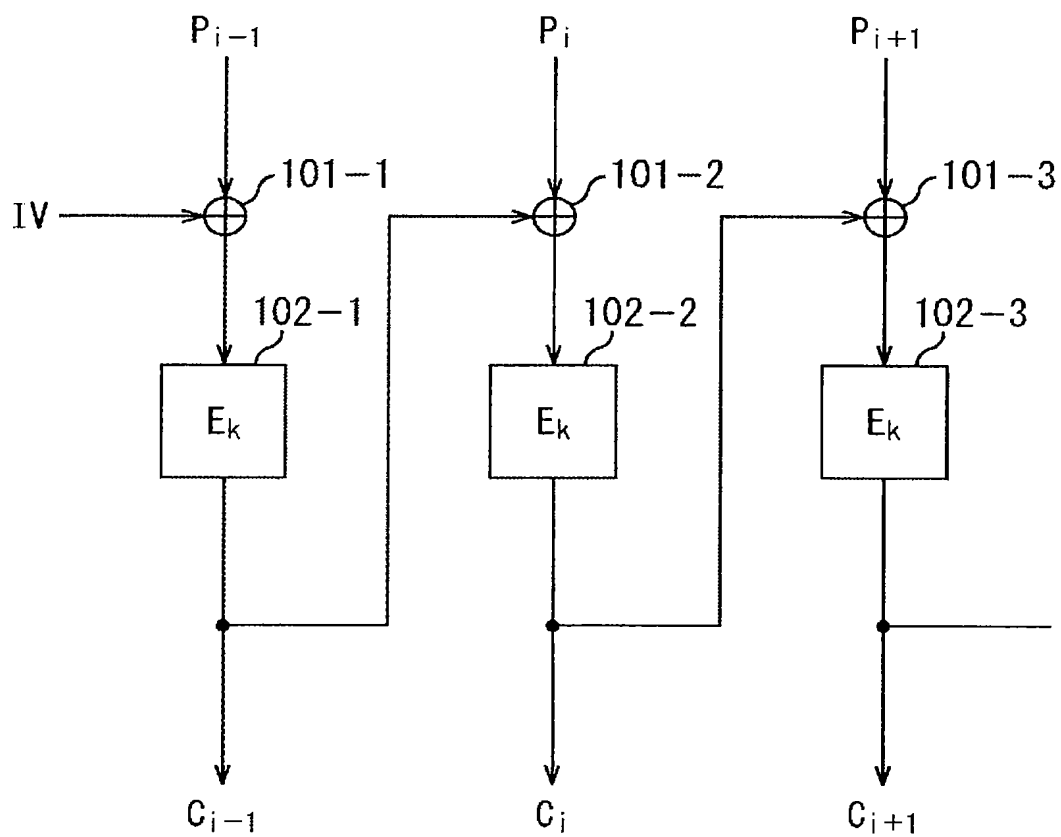
[図3]

図3



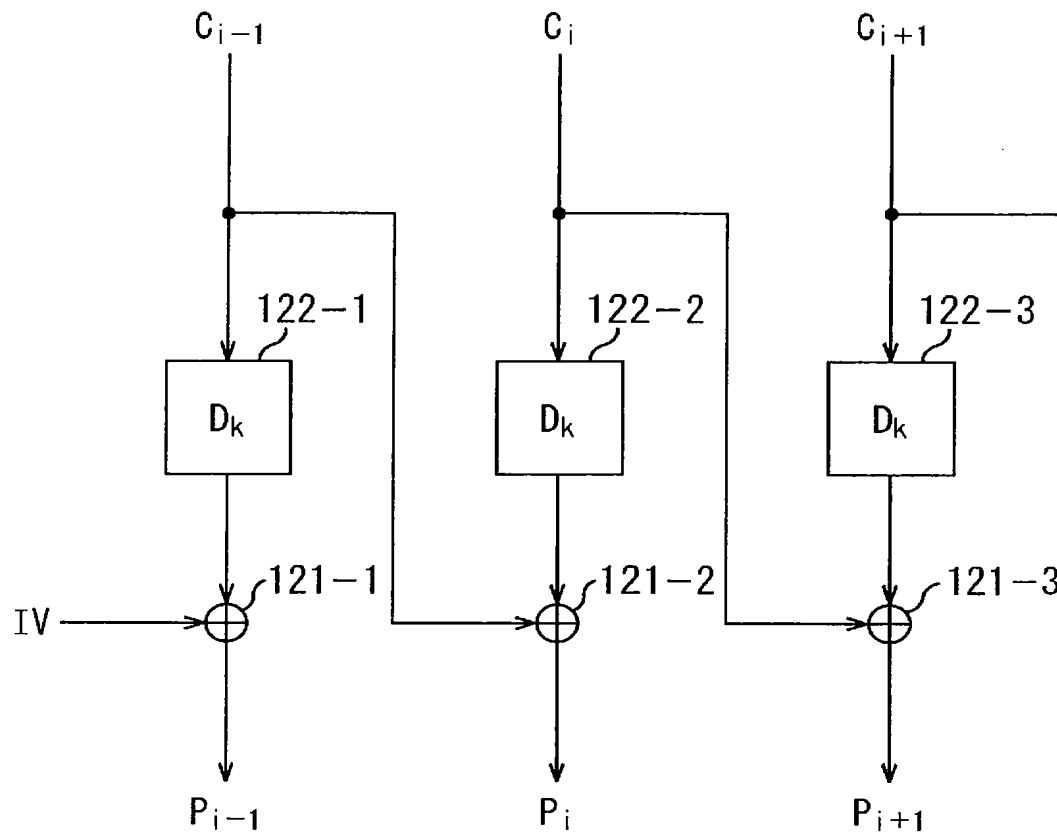
[図4]

図4



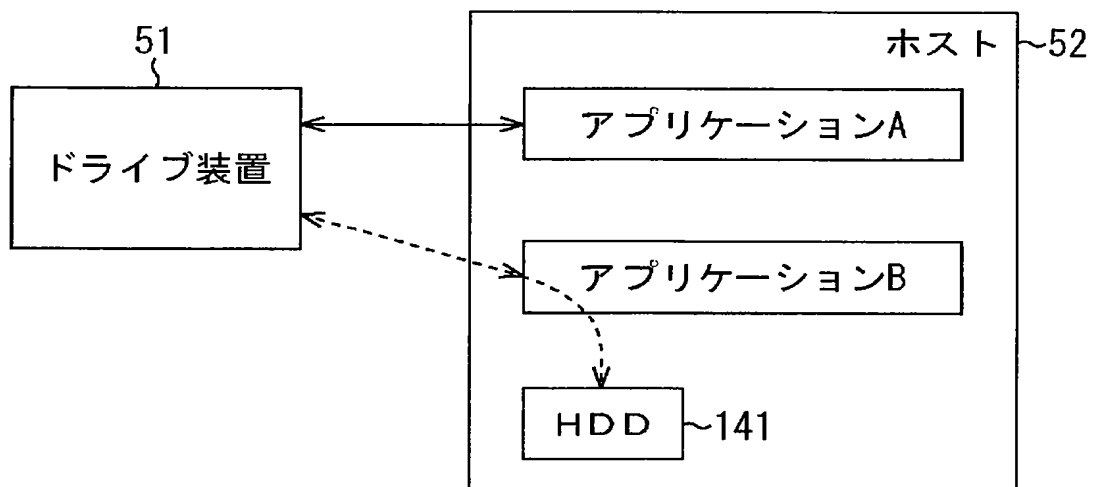
[図5]

図5



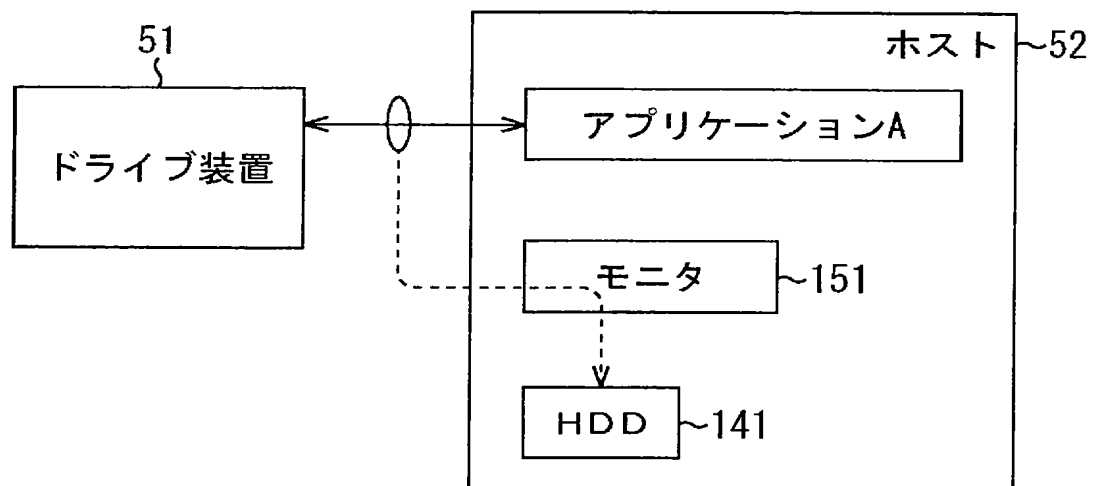
[図6]

図6



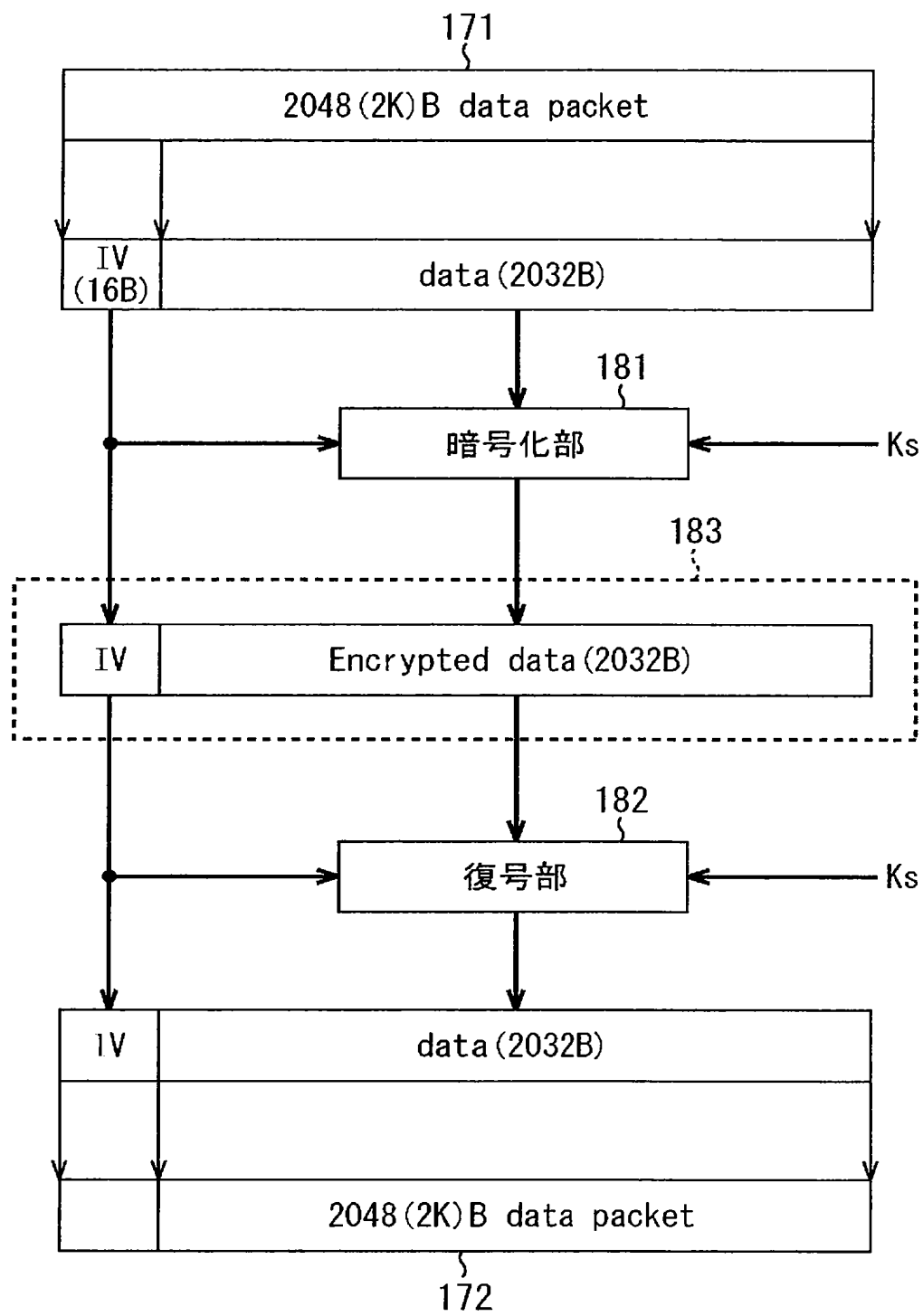
[図7]

図7



[図8]

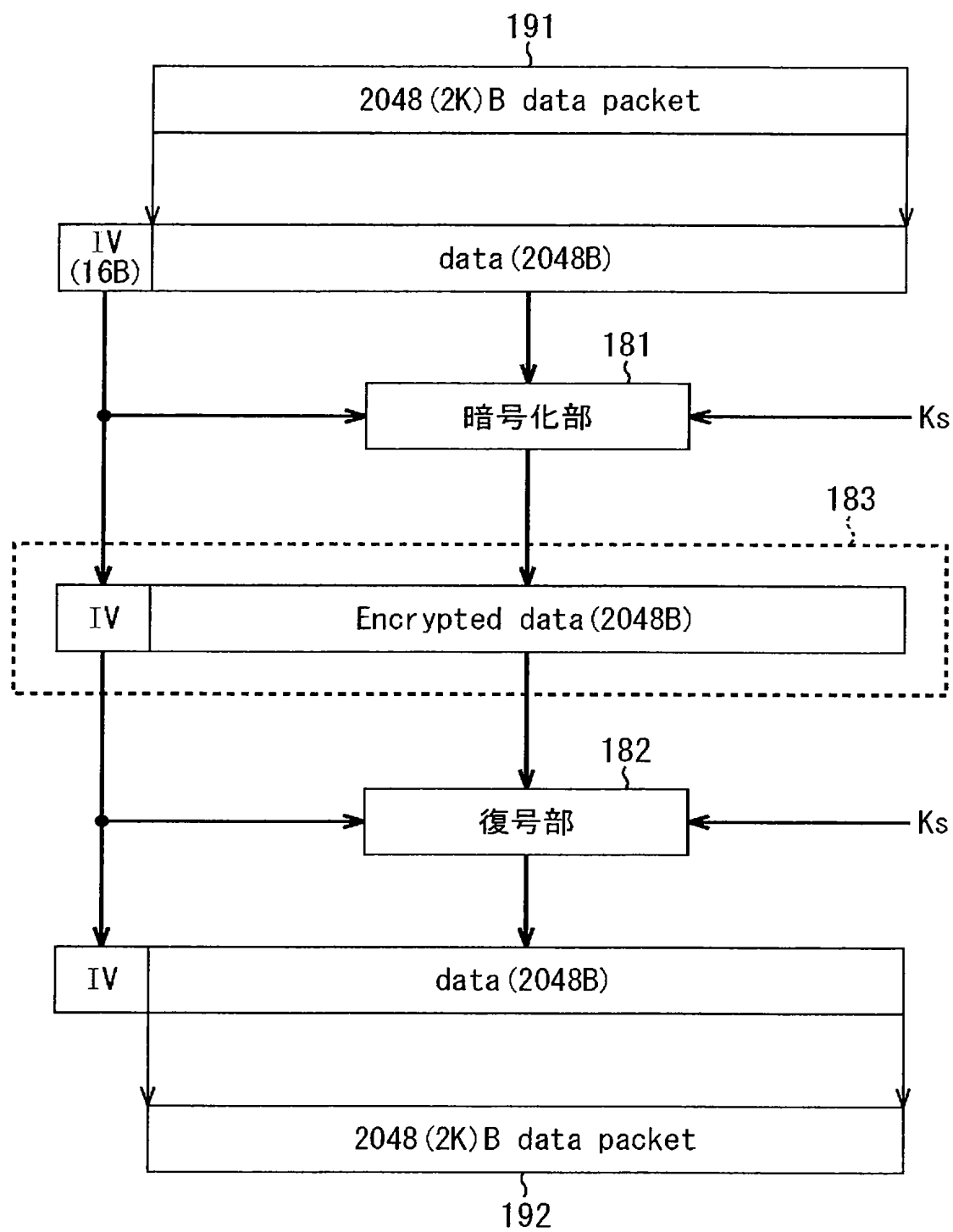
図8





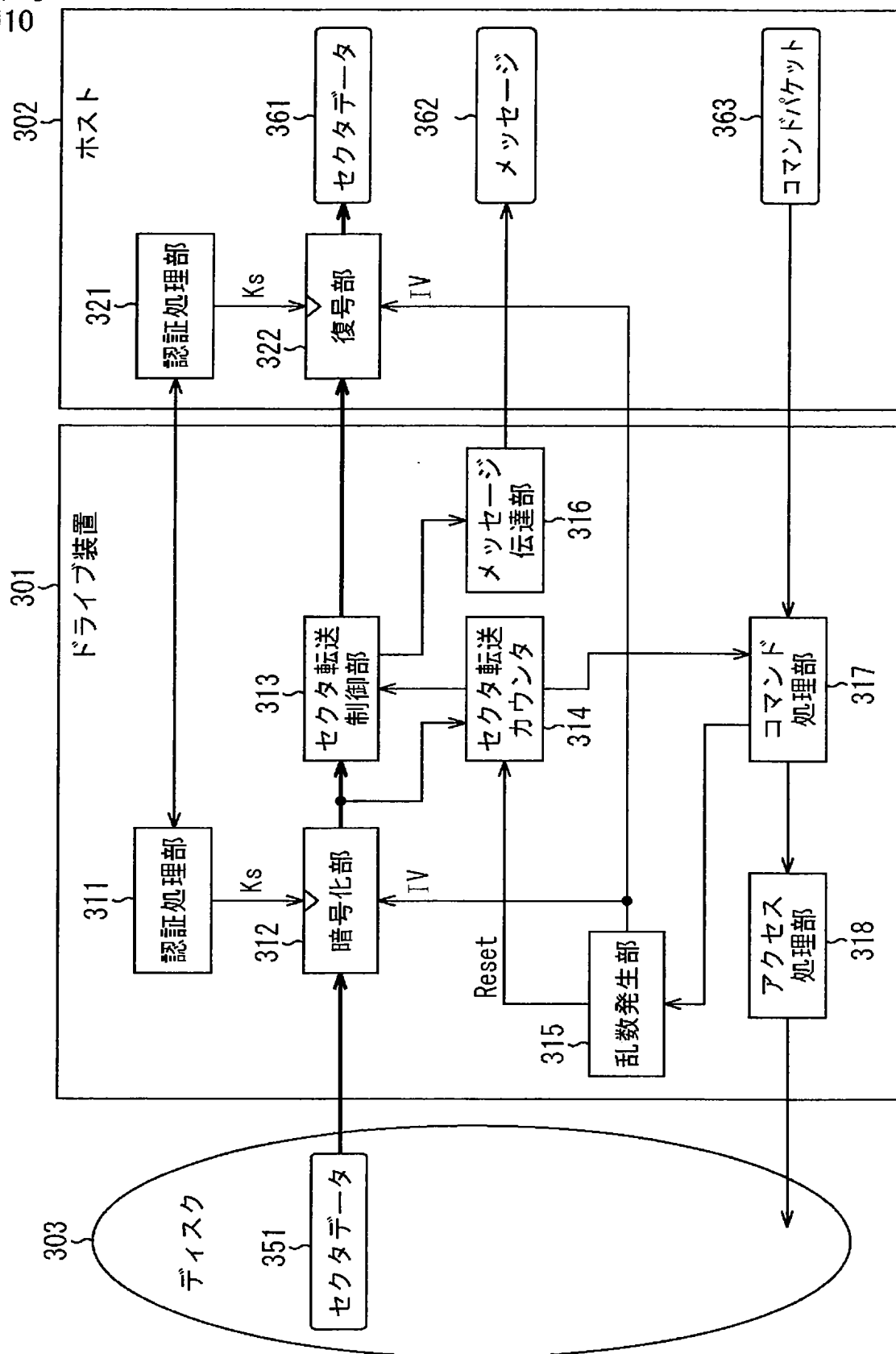
[図9]

図9

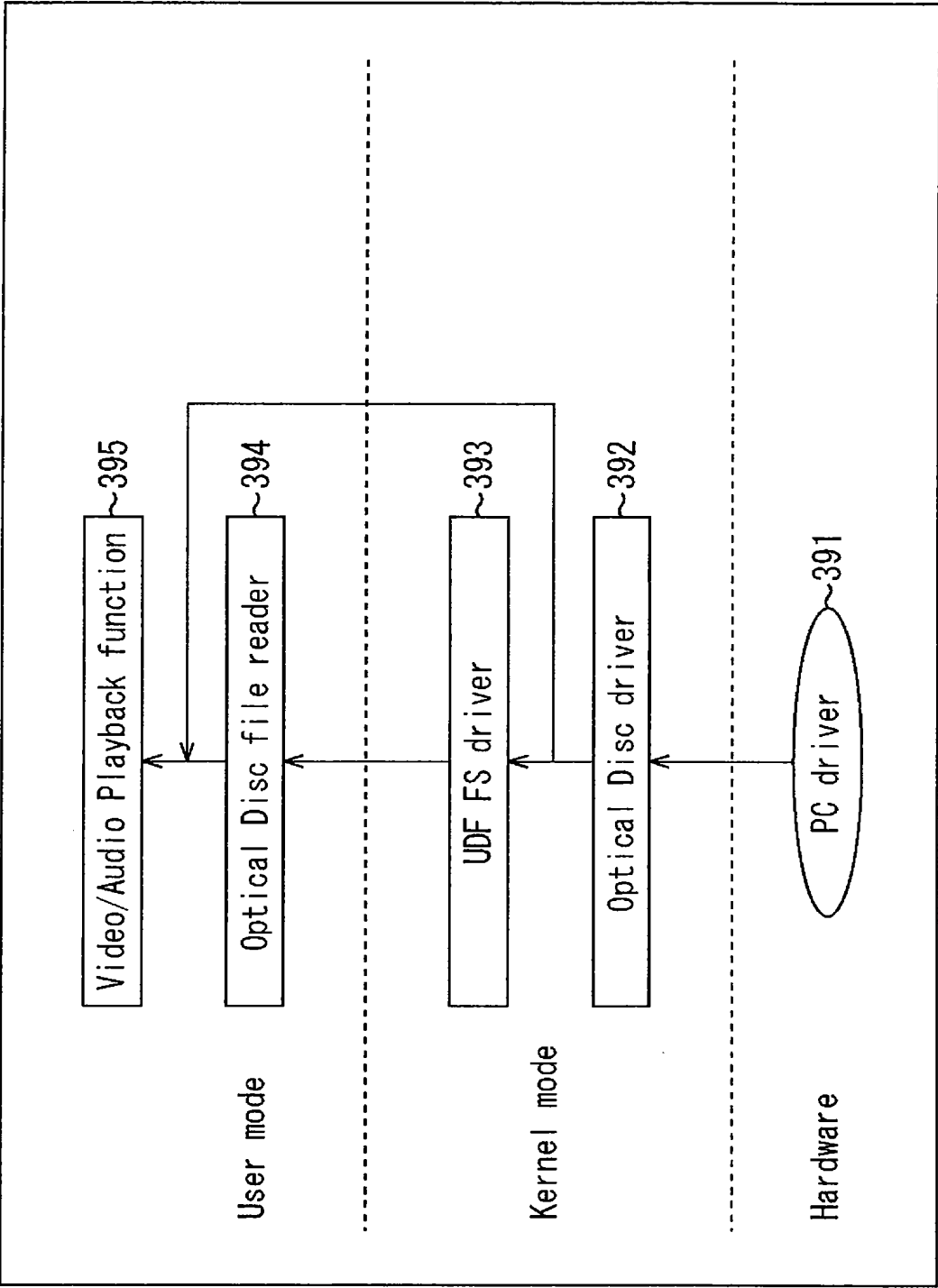


[図10]

図10



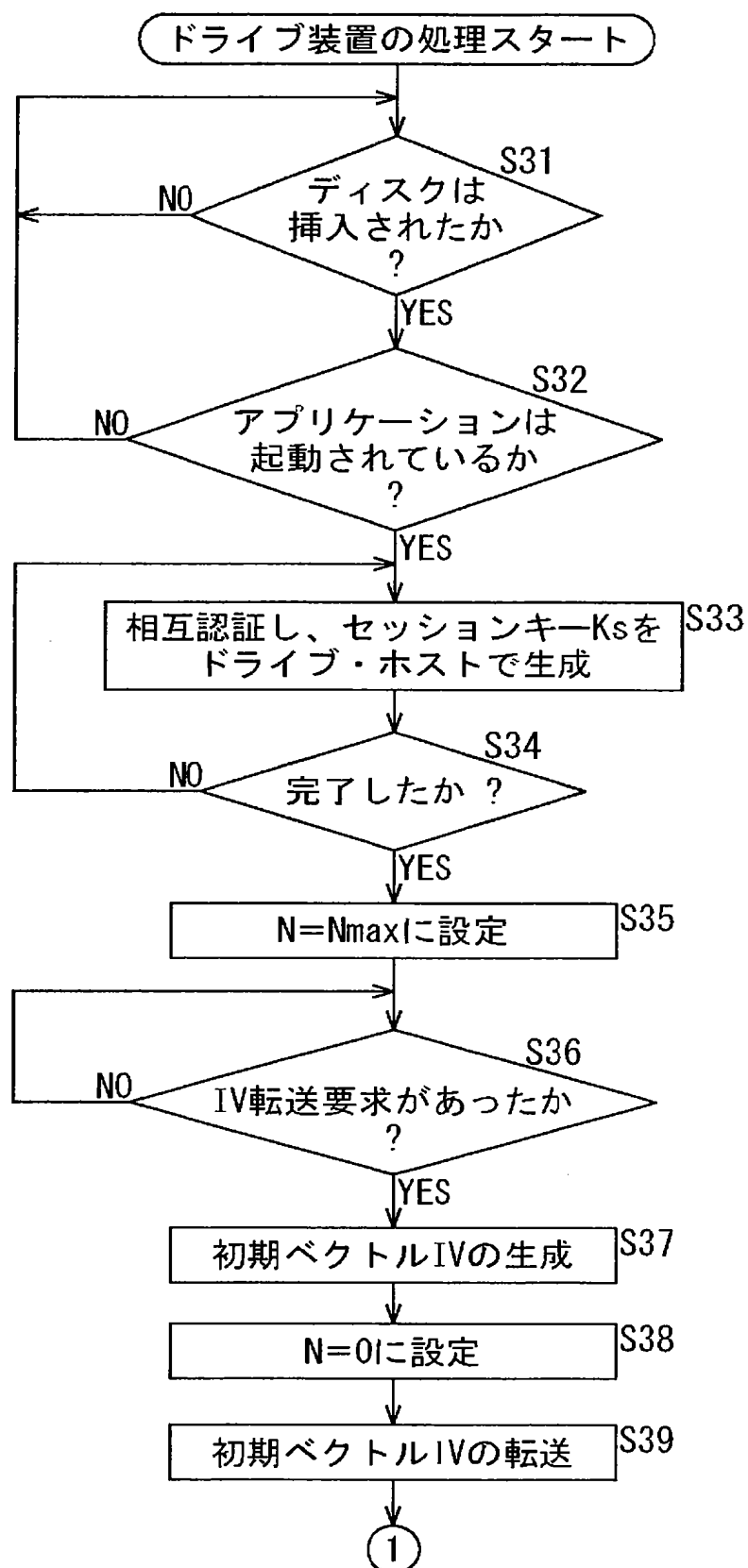
[図11]  
図11



[図12]

図12

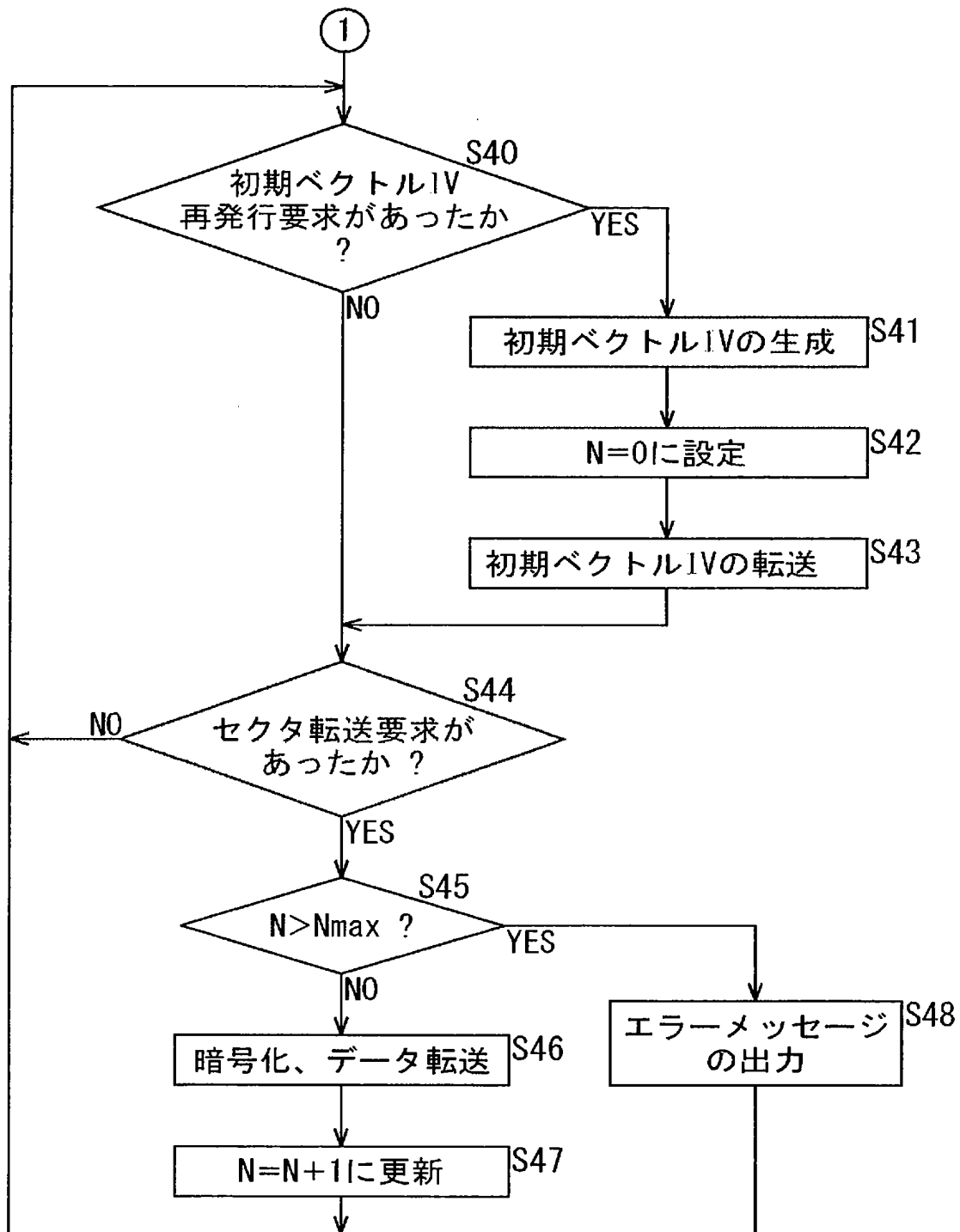
(12-1)



[図13]

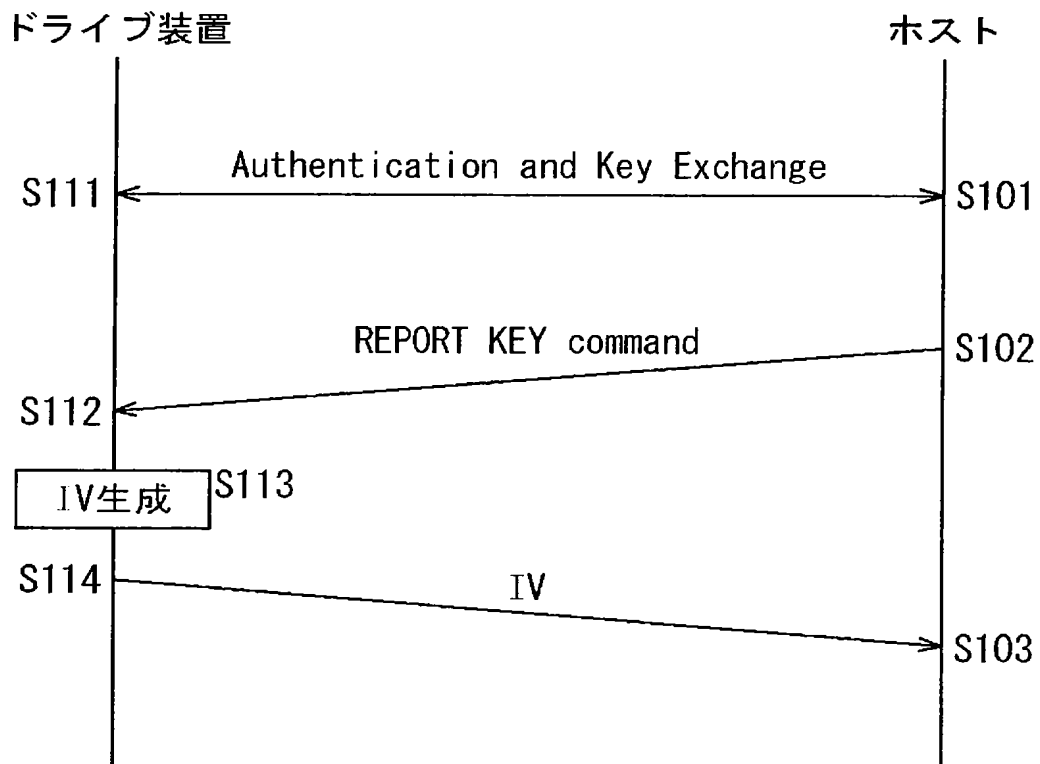
図13

(12-2)



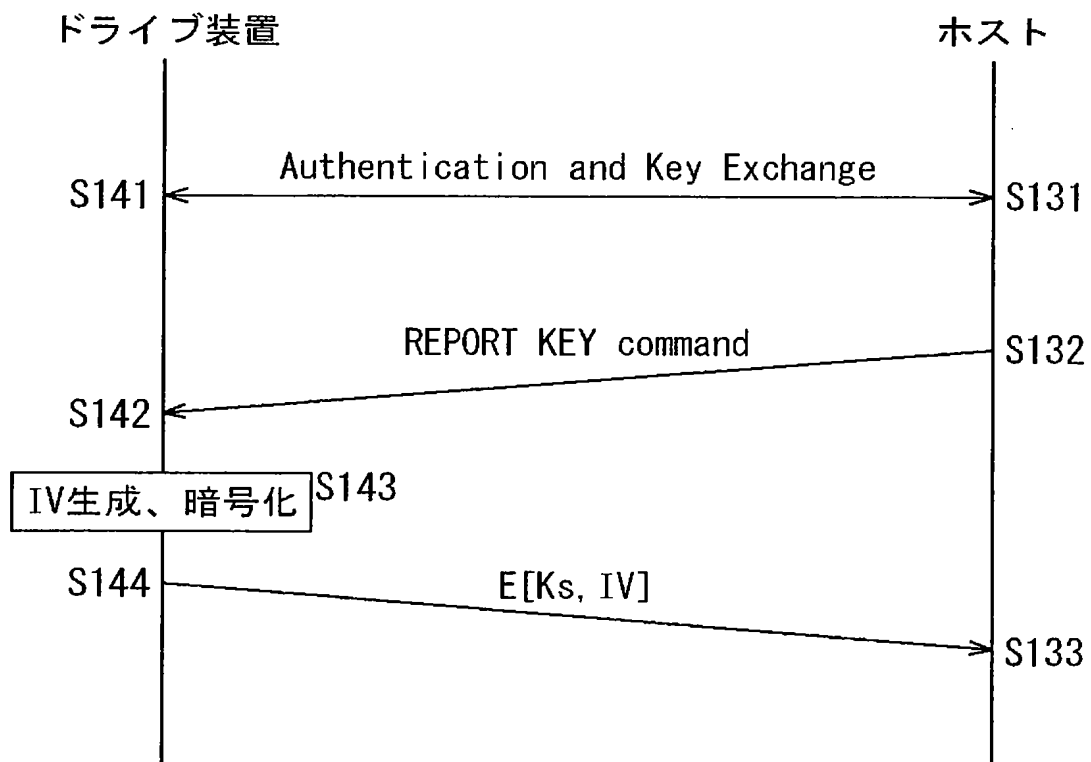
[図14]

図14



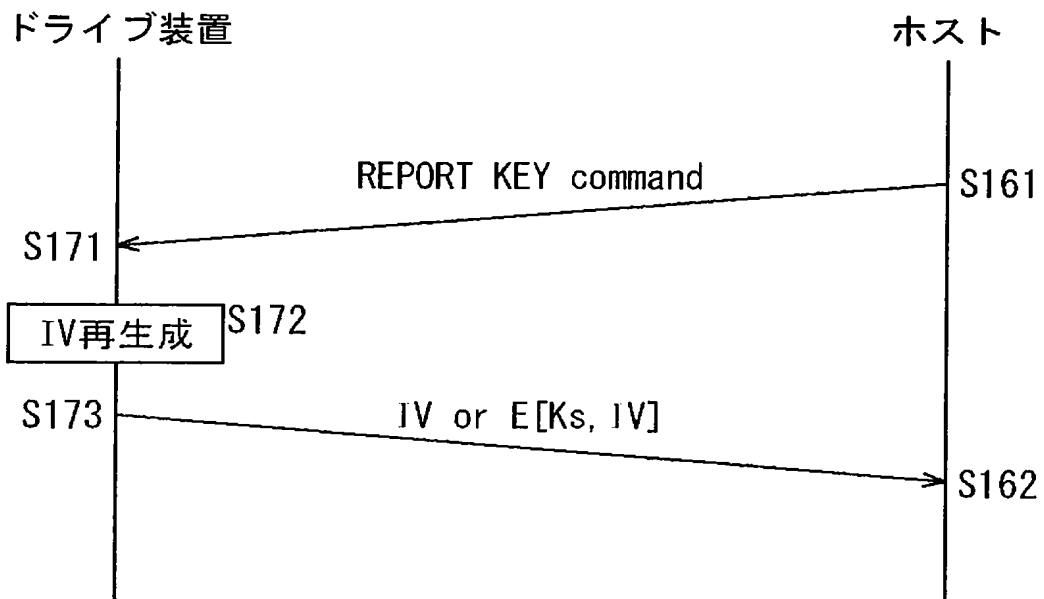
[図15]

図15



[図16]

図16





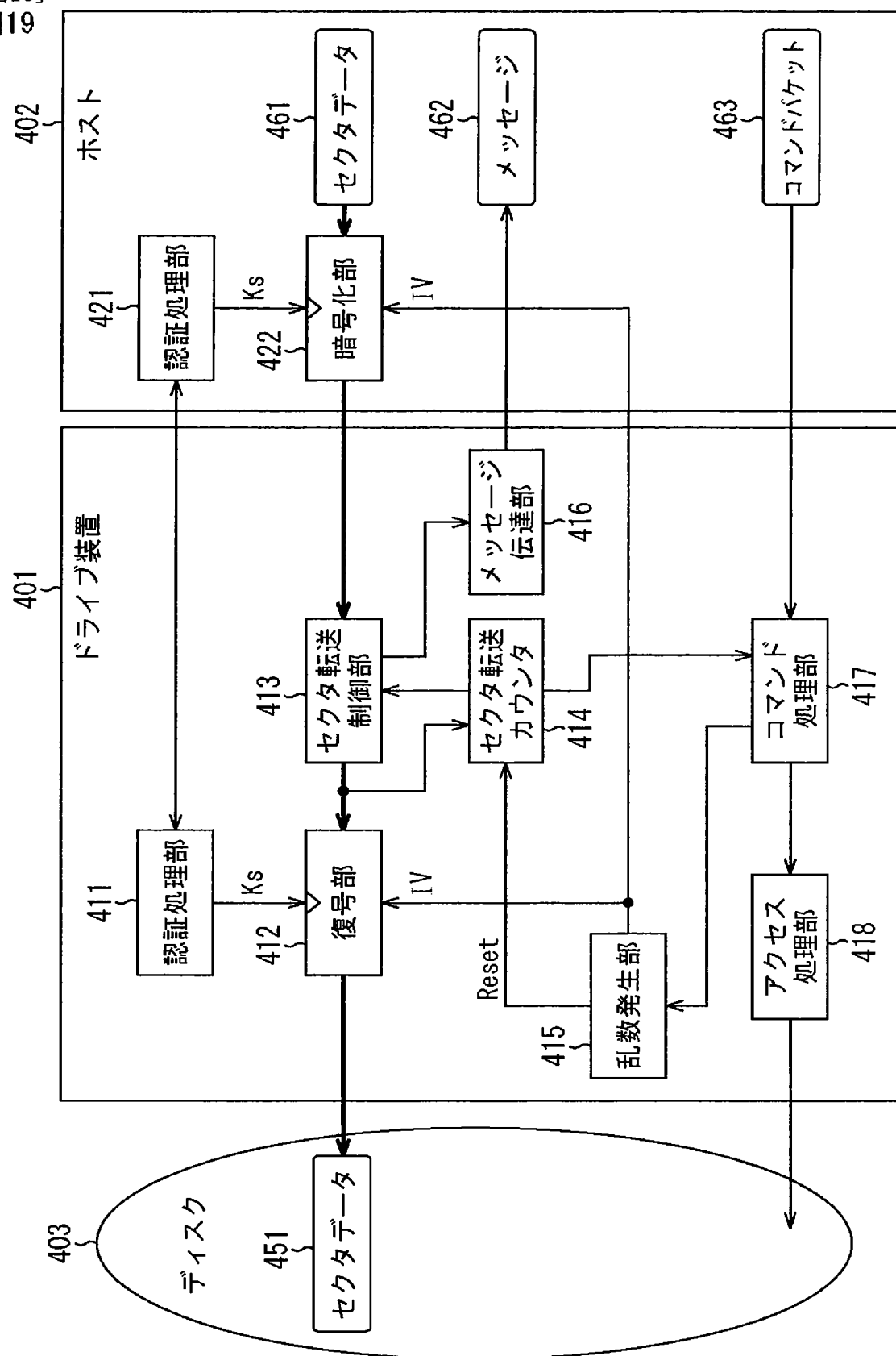


[ 18]  
[ 18]

Bit		7	6	5	4	3	2	1	0
Byte									
0		Operation Code							
1		LUN (Obsolete)				DPO (0)	FUA	Reserved	Re Adr
2		Logical Block Address							
3									
4									
5									
6		Transfer Length							
7									
8									
9									
10		Streaming	Reserved						
11		Vendor-Specific		Reserved			NACA	Flag	Link

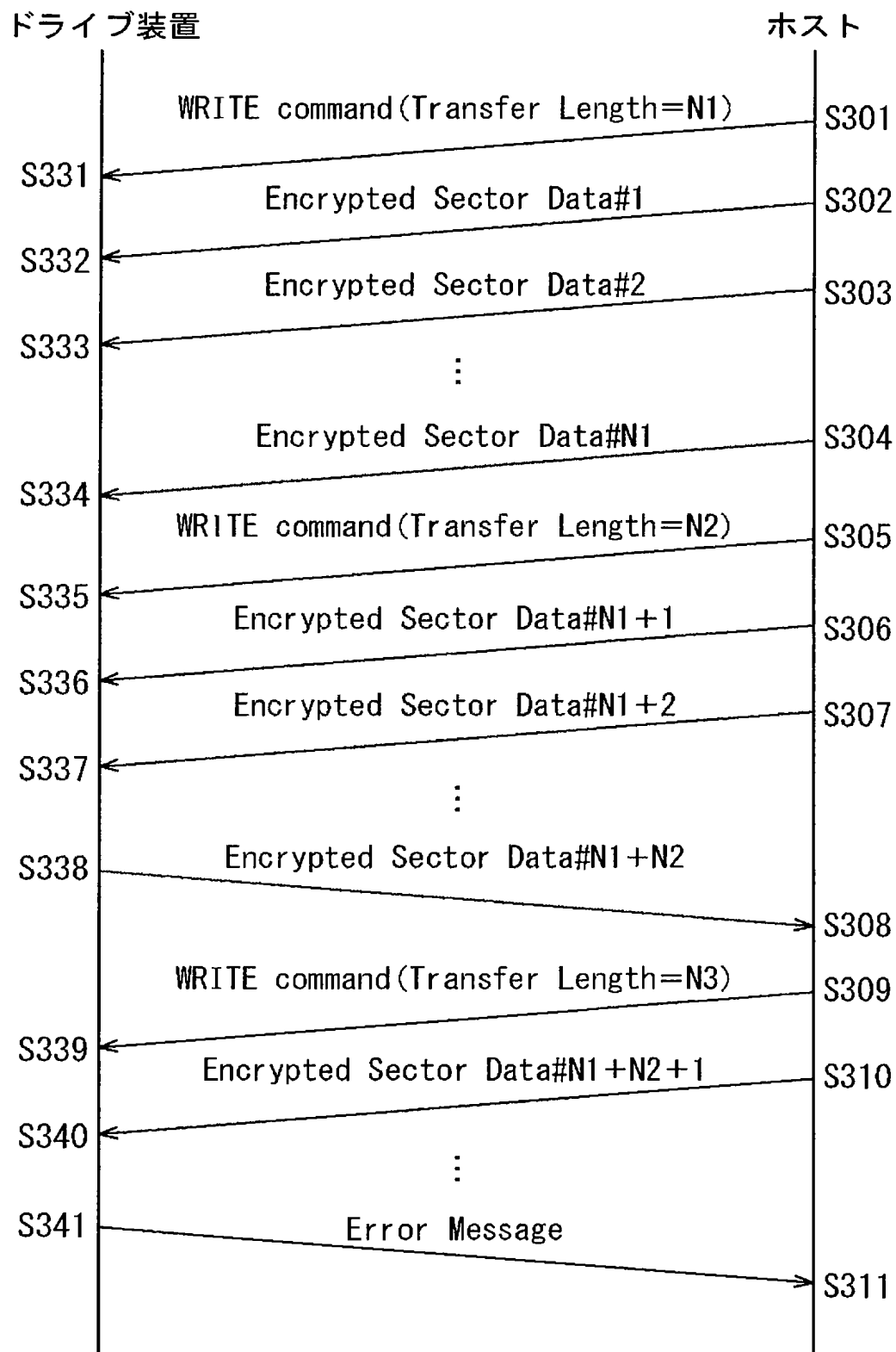
[図19]

図19

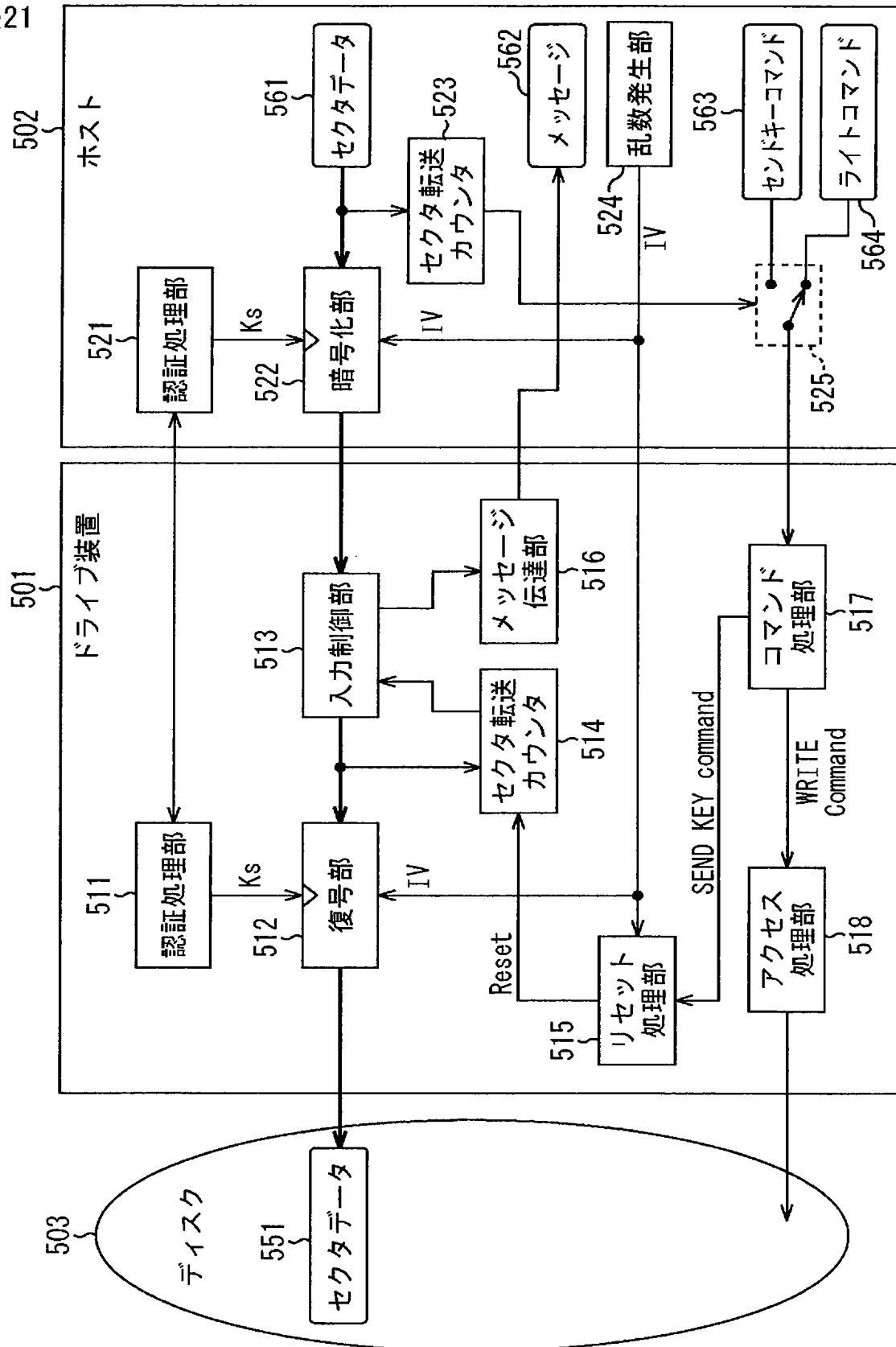


[図20]

図20

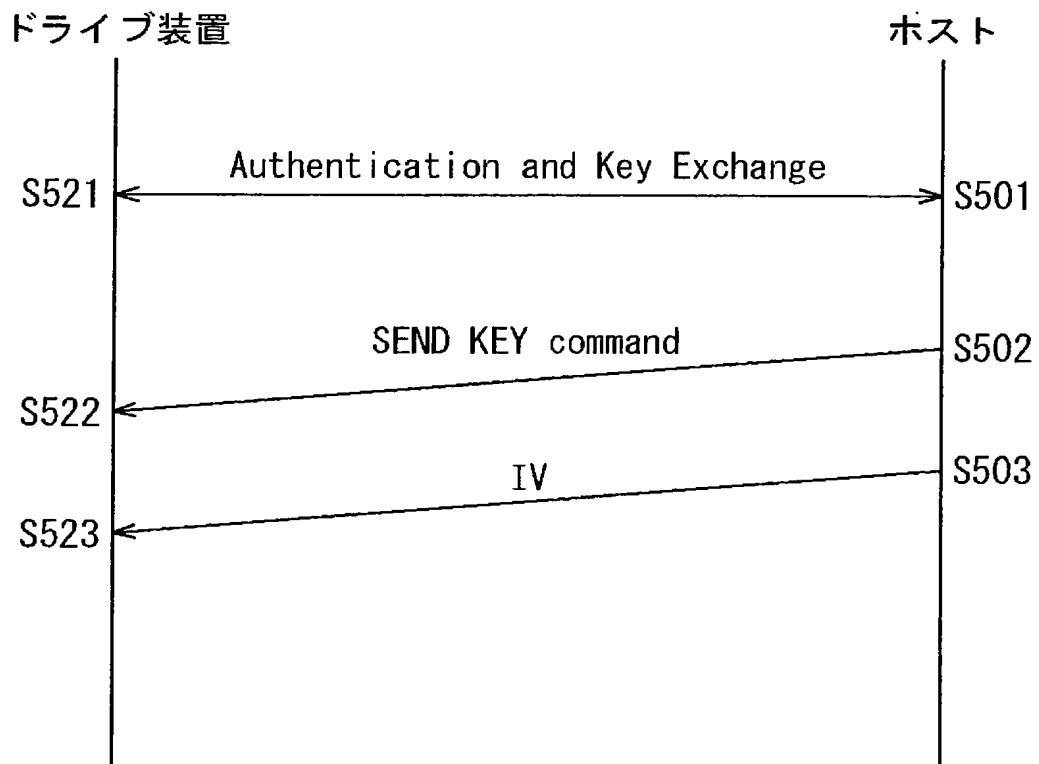


[図21]  
図21



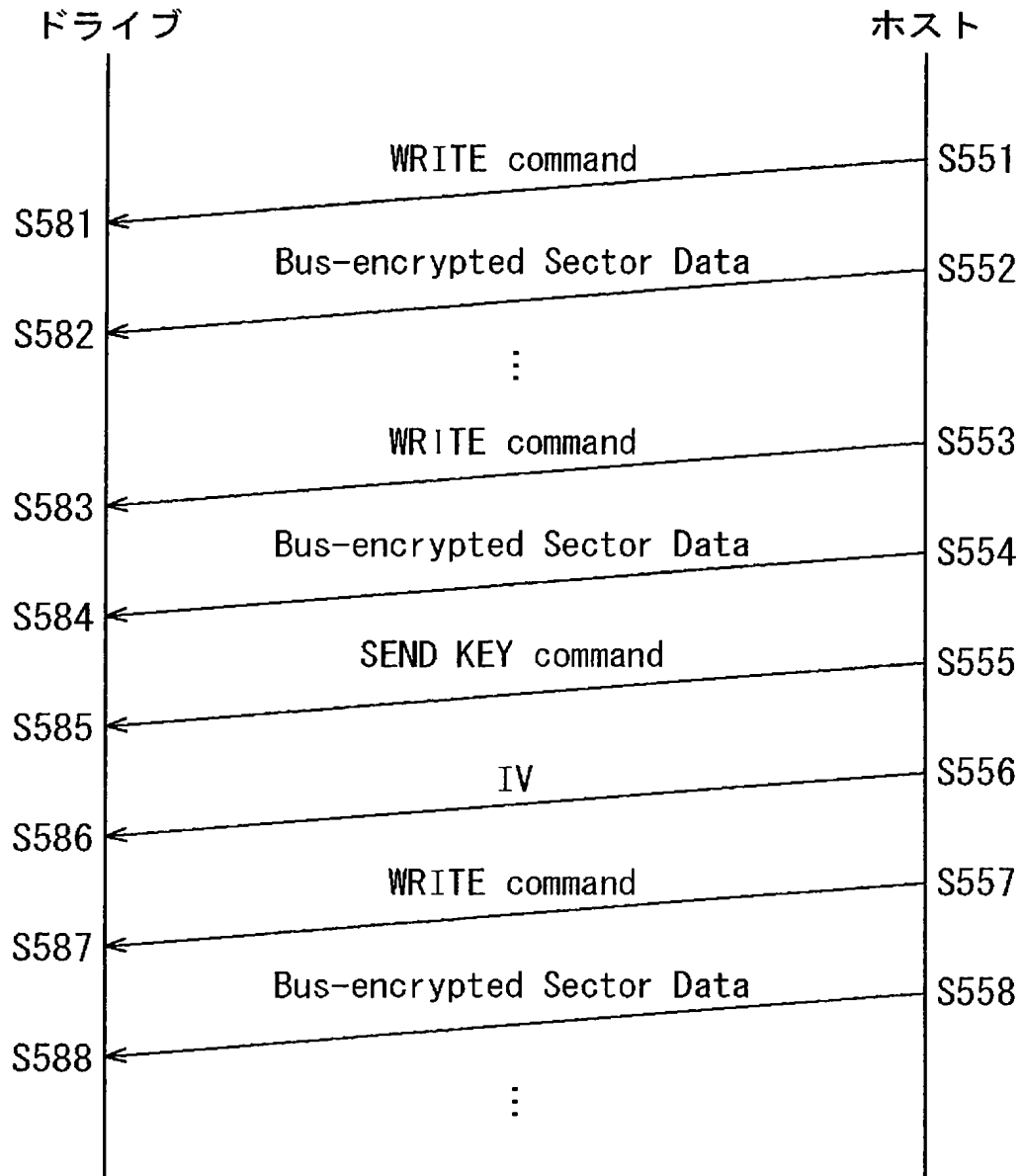
[図22]

図22



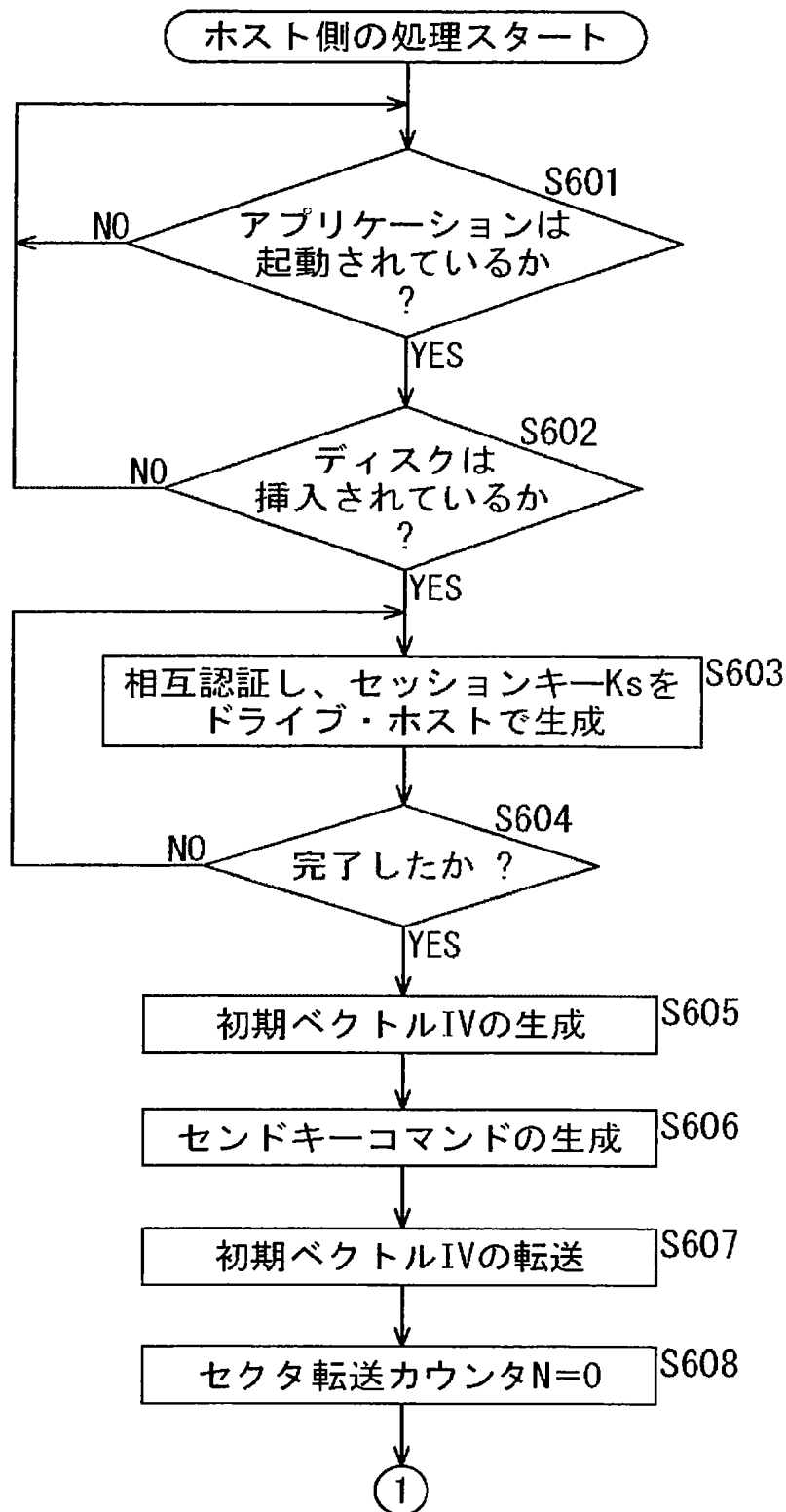
[図23]

図23



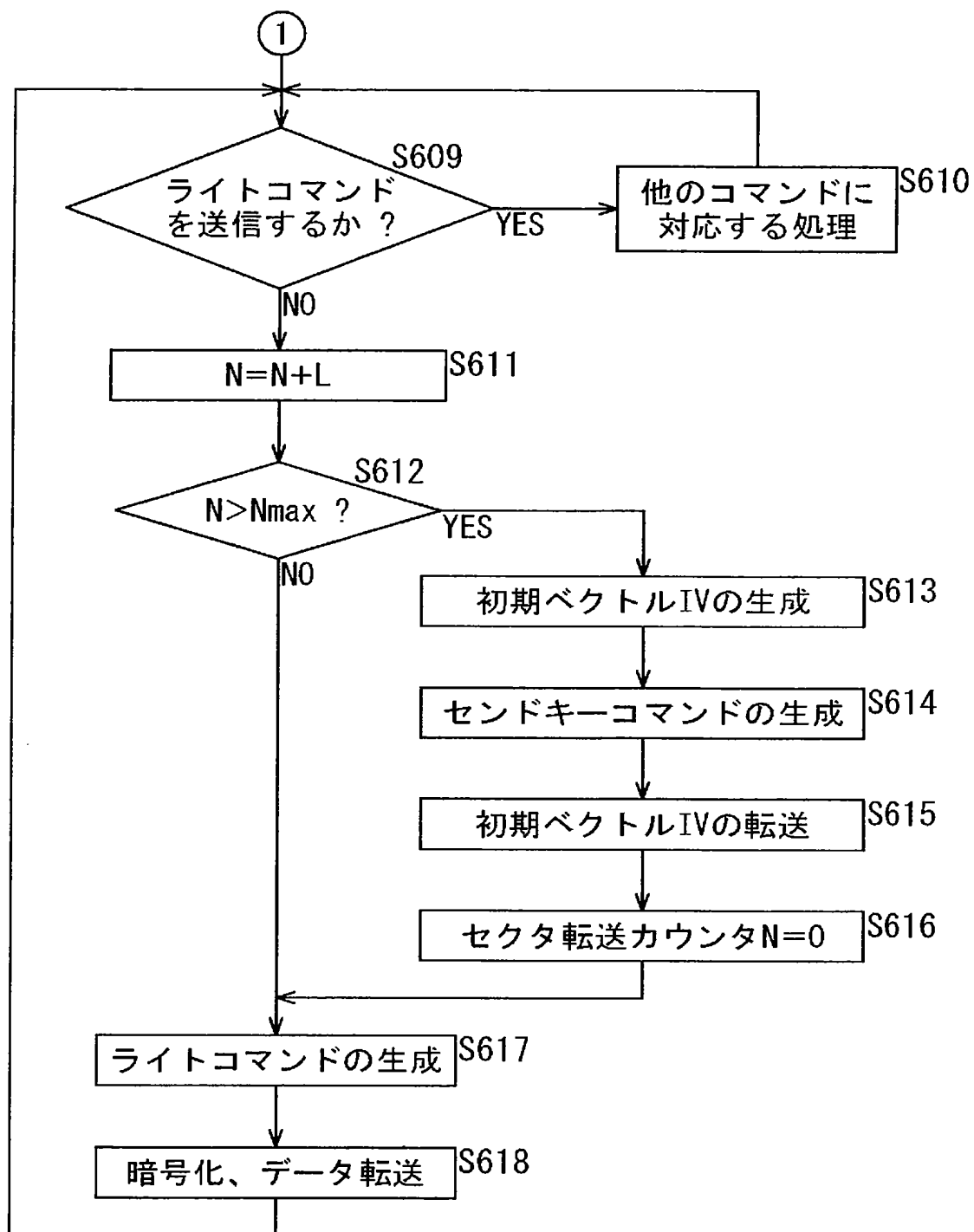
[図24]

図24



[図25]

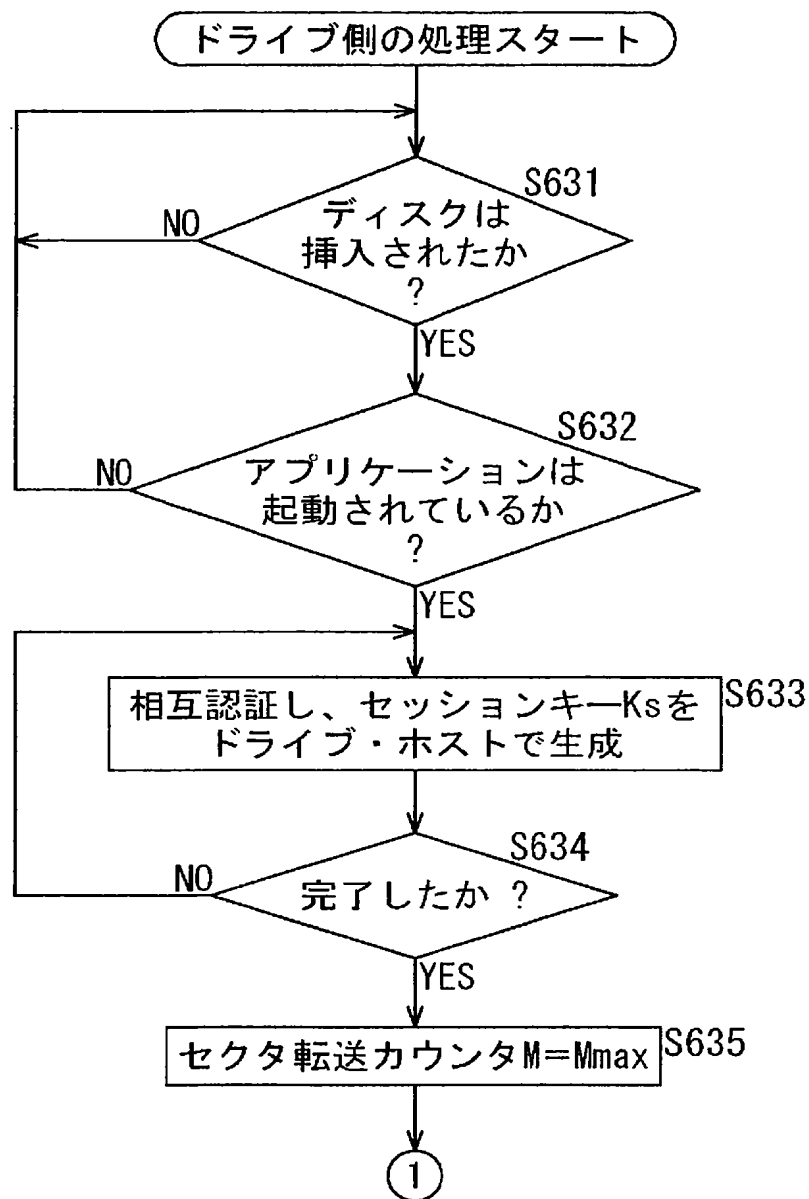
図25





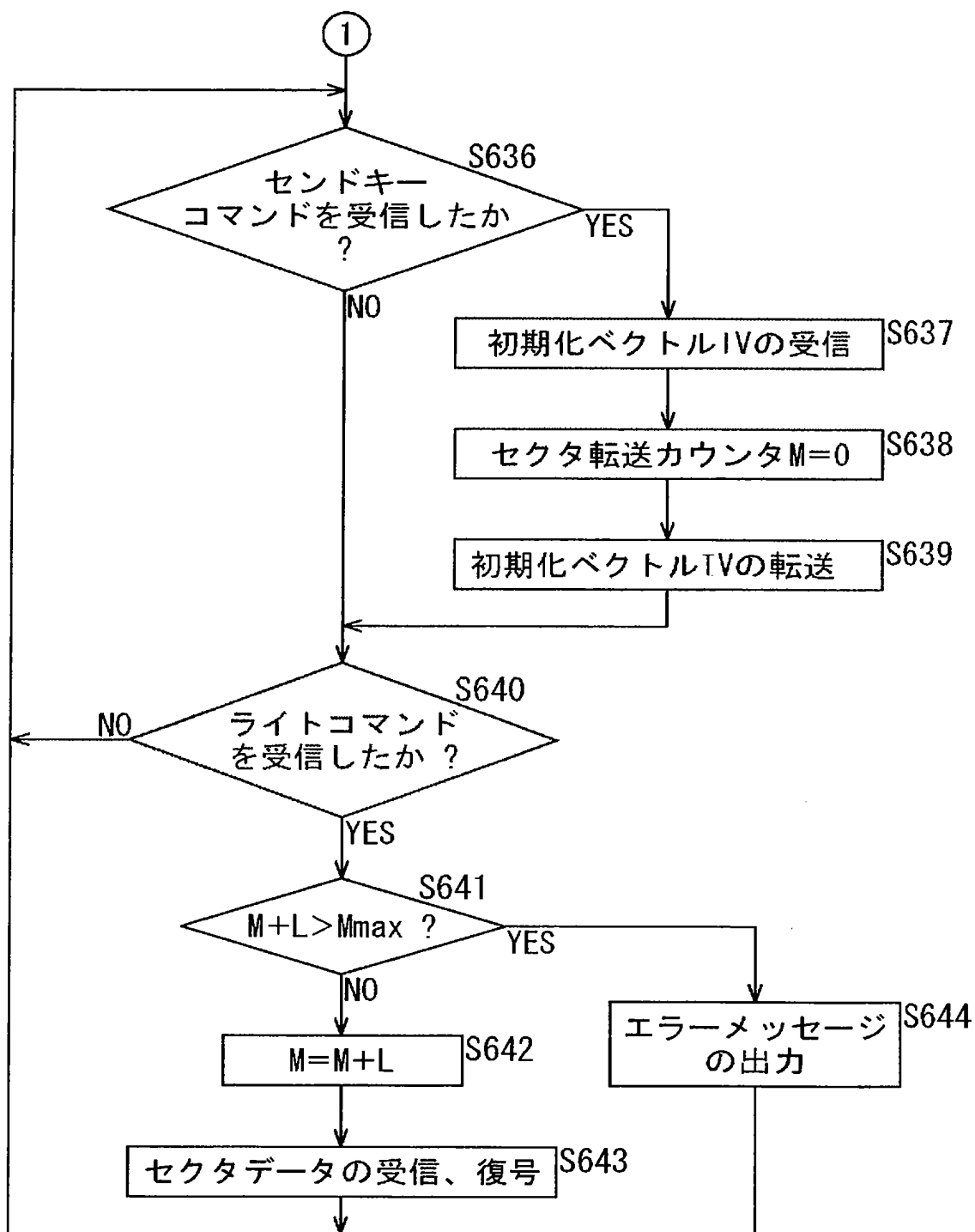
[図26]

図26



[図27]

図27



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/000061

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.<sup>7</sup> H04L9/08, H04L9/16, G06F12/14, G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.<sup>7</sup> H04L9/08, H04L9/16, G06F12/14, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Jitsuyo Shinan Toroku Koho	1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2003/034425 A (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 24 April, 2003 (24.04.03), Full text & JP 2005-505873 A	1-5
A	JP 2001-521697 A (DEUTSCHE TELEKOM AG.), 06 November, 2001 (06.11.01), Full text & WO 98/048540 A	1-5
A	JP 2001-306401 A (Matsushita Electric Industrial Co., Ltd.), 02 November, 2001 (02.11.01), Full text & WO 2001/052474 A	1-5

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier application or patent but published on or after the international filing date  
 "I" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
15 March, 2005 (15.03.05)

Date of mailing of the international search report  
29 March, 2005 (29.03.05)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/000061

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-330872 A (Sony Corp.), 30 November, 2000 (30.11.00), Full text & EP 1037209 A	1-5
A	JP 10-65662 A (Sony Corp.), 06 March, 1998 (06.03.98), Full text & US 5883958 A	1-5
A	JP 8-335040 A (Fujitsu Ltd.), 17 December, 1996 (17.12.96), Full text & US 6460137 B1	1-5

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L9/16, G06F12/14, G11B20/10

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L9/16, G06F12/14, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2005年

日本国登録実用新案公報 1994-2005年

日本国実用新案登録公報 1996-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	WO 2003/034425 A (KONINKLIJKE PHILIPS ELECTRONICS N.V.) 2003. 04. 24, 全文 & JP 2005-505873 A	1-5
A	JP 2001-521697 A (ドイッチェ テレコム アーゲー) 2001. 11. 06, 全文 & WO 98/048540 A	1-5

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願口又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」同一パテントファミリー文献

国際調査を完了した日

15. 03. 2005

国際調査報告の発送日

29. 3. 2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行

5M

9469

電話番号 03-3581-1101 内線 3598

## C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2001-306401 A (松下電器産業株式会社) 2001. 11. 02, 全文 & WO 2001/052474 A	1-5
A	JP 2000-330872 A (ソニー株式会社) 2000. 11. 30, 全文 & EP 1037209 A	1-5
A	JP 10-65662 A (ソニー株式会社) 1998. 03. 06, 全文 & US 5883958 A	1-5
A	JP 8-335040 A (富士通株式会社) 1996. 12. 17, 全文 & US 6460137 B1	1-5